SALEM NUMBERS AND ARITHMETIC HYPERBOLIC GROUPS

VINCENT EMERY, JOHN G. RATCLIFFE AND STEVEN T. TSCHANTZ

Abstract. In this paper we prove that there is a direct relationship between Salem numbers and translation lengths of hyperbolic elements of arithmetic hyperbolic groups that are determined by a quadratic form over a totally real number field.

1. Introduction

In this paper, a *Salem number* is a real algebraic integer $\lambda > 1$ that is conjugate to λ^{-1} and whose remaining conjugates lie on the unit circle. Salem numbers are of interest in many areas of mathematics including Diophantine analysis, harmonic analysis, dynamical systems, Coxeter groups, Fuchsian groups, knot theory, and K3 surfaces. For surveys on Salem numbers, see [12] and [28].

Let λ be an algebraic integer, let K be a number field, and let $\deg_K(\lambda)$ be the degree of the minimal polynomial of λ over K. The *degree* of λ is $\deg_{\mathbb{Q}}(\lambda)$. Salem numbers have even degree, and there are Salem numbers of every positive even degree. Usually Salem numbers have degree at least 4. However, we will allow Salem numbers of degree 2 for uniformity of terminology. Note that a Salem number λ has degree 2 if and only if $\lambda + \lambda^{-1} \in \mathbb{Z}$.

Arithmetic hyperbolic groups are arithmetic groups of isometries of hyperbolic n-space H^n. The arithmetic hyperbolic groups of the simplest type are defined in terms of an admissible quadratic form over a totally real number field K on p. 217 of [30]. The arithmetic hyperbolic groups of the simplest type form a large class of arithmetic hyperbolic groups that includes all arithmetic hyperbolic groups in even dimensions [30], infinitely many wide-commensurability classes of arithmetic hyperbolic groups in all dimensions [20], and all non-cocompact arithmetic hyperbolic groups in all dimensions [19].

There are three types of isometries of H^n, namely *elliptic, parabolic*, and *hyperbolic* isometries. An isometry γ of H^n is *hyperbolic* if and only if there is a unique geodesic L in H^n, called the *axis* of γ, along which γ acts as a translation by a positive distance $\ell(\gamma)$ called the *translation length* of γ.

If Γ is an arithmetic group of isometries of H^n, then Γ is a discrete group of isometries of H^n which has finite covolume if $n > 1$. If Γ is a discrete group of isometries of H^n of finite covolume, then Γ contains a hyperbolic isometry and most elements of Γ are hyperbolic.

Let γ is a hyperbolic element of a discrete group Γ of isometries of H^n. The axis L of γ projects to a closed geodesic C in the hyperbolic orbifold H^n/Γ. The translation length of γ is a multiple of the length of C and equals the length of C if

1991 *Mathematics Subject Classification.* 11E10, 11F06, 11R06, 20F55, 30F40.

Key words and phrases. arithmetic group, closed geodesic, hyperbolic group, quadratic form, Salem number, totally real number field.

and only if γ is a primitive element of Γ, that is, γ is not a proper power of another element of Γ. Every hyperbolic element of Γ is a power of a primitive hyperbolic element of Γ. Hence the set of lengths of closed geodesics in H^n/Γ is the set of translation lengths of primitive hyperbolic elements of Γ.

In this paper, we show that Salem numbers are directly related to the translation lengths of hyperbolic elements of an arithmetic hyperbolic group of the simplest type. Our main results are Theorems 1 and 2 below which sharpen and generalizes to all dimensions results obtained by T. Chinburg, W. Neumann and A. Reid [23] in dimension 2 and 3.

Theorem 1. *Let Γ be an arithmetic group of isometries of hyperbolic n-space H^n, with $n > 1$, of the simplest type defined over a totally real number field K, and let $\Gamma^{(2)}$ be the subgroup of Γ of finite index generated by the squares of elements of Γ. Let γ be a hyperbolic element of Γ, and let $\lambda = e^{\ell(\gamma)}$. If n is even or $\gamma \in \Gamma^{(2)}$, then λ is a Salem number such that $K \subseteq \mathbb{Q}(\lambda + \lambda^{-1})$ and $\deg_K(\lambda) \leq n + 1$.*

Conversely, if λ is a Salem number, and K is a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, and n is a positive integer such that $\deg_K(\lambda) \leq n + 1$, then there exists an arithmetic group Γ of isometries of H^n of the simplest type defined over K and a hyperbolic element γ in Γ such that $\lambda = e^{\ell(\gamma)}$.

Note that $\deg \lambda = 2$ in Theorem 1 only if $K = \mathbb{Q}$. Theorem 1 has the following corollary with no restriction on dimension.

Corollary 1. *Let λ be a Salem number. Then for each positive integer n, there exists an arithmetic group Γ of isometries of H^n of the simplest type defined over $\mathbb{Q}(\lambda + \lambda^{-1})$ and a hyperbolic element γ of Γ such that $\lambda = e^{\ell(\gamma)}$.*

The set $\mathcal{S}_d$ of Salem numbers of degree d has a least element by Lemma 3 of [12]. All non-cocompact arithmetic hyperbolic groups are arithmetic hyperbolic groups of the simplest type defined over $\mathbb{Q}$ [19]. For each positive integer n, let

$$b_n = \min\{\log \lambda : \lambda \text{ is a Salem number with } \deg \lambda \leq n + 1\}.$$

The next corollary follows from Theorem 1 and a sharp example for $n = 2$.

Corollary 2. *If Γ is a non-cocompact arithmetic group of isometries of H^n, with n even, and C is a closed geodesic in H^n/Γ, then* $\mathrm{length}(C) \geq b_n$, *and this lower bound is sharp for each even integer $n > 0$.*

Let λ be a Salem number, and let K be a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, and let $p(x)$ be the minimal polynomial of λ over K. We say that λ is *square-rootable over K* if there exists a totally positive element α of K and a monic palindromic polynomial $q(x)$, whose even degree coefficients are in K and whose odd degree coefficients are in $\sqrt{\alpha}K$, such that $q(x)q(-x) = p(x^2)$.

Theorem 2. *Let Γ be an arithmetic group of isometries of hyperbolic n-space H^n, with n odd and $n > 1$, of the simplest type defined over a totally real number field K. Let γ be a hyperbolic element of Γ, and let $\lambda = e^{2\ell(\gamma)}$. Then λ is a Salem number which is square-rootable over K.*

Conversely, if λ is a Salem number and K is a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, and n is an odd positive integer such that $\deg_K(\lambda) \leq n + 1$, and λ is square-rootable over K, then there exists an arithmetic group Γ of isometries of H^n of the simplest type defined over K and a hyperbolic element γ in Γ such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$.

Any Salem number λ is square-rootable over $\mathbb{Q}(\lambda + \lambda^{-1})$, and so Theorem 2 implies the next Corollary, which improves Corollary 1 in odd dimensions.

Corollary 3. *Let λ be a Salem number. Then for each odd integer $n > 0$, there exists an arithmetic group Γ of isometries of H^n of the simplest type defined over $\mathbb{Q}(\lambda + \lambda^{-1})$ and a hyperbolic element γ of Γ such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$.*

For each positive integer n, let

$$\begin{aligned} c_n \;\; = \;\; & \min\{\tfrac{1}{2}\log\lambda : \lambda \text{ is a Salem number with } \deg\lambda \leq n+1, \\ & \qquad \text{which is square-rootable over } \mathbb{Q}\}. \end{aligned}$$

The next corollary follows from Theorem 2 and a sharp example for $n = 3$.

Corollary 4. *If Γ is a non-cocompact arithmetic group of isometries of H^n, with n odd and $n > 1$, and C is a closed geodesic in H^n/Γ, then* $\mathrm{length}(C) \geq c_n$*, and this lower bound is sharp for each odd integer $n > 1$.*

Our lower bound, $c_3 = .431277\ldots$, for the length of a closed geodesic in an arithmetic, noncompact, hyperbolic 3-orbifold H^3/Γ agrees with the lower bound given in [23]. We thank Alan Reid for helpful correspondence in this regard.

We say that Salem numbers λ and μ are *commensurable* if there exists positive integers k and ℓ such that $\lambda^k = \mu^\ell$. Commensurability is an equivalence relation on the set of all Salem numbers. We also prove the following theorem.

Theorem 3. *Let Γ be an arithmetic group of isometries of hyperbolic n-space H^n, with $n > 1$, of the simplest type defined over a totally real number field K. Then there exists infinitely many commensurability classes of Salem numbers of the form $e^{\ell(\gamma)}$ for some hyperbolic element γ of Γ.*

Our paper is organized as follows: In §2, we present background material for the paper. In §3, we prove some preliminary algebraic lemmas. In §4, we prove some linear algebraic group lemmas. In §5, we prove the first half of Theorem 1. In §6, we prove Theorem 3. In §7, we prove the second half of Theorem 1. In §8, we prove Theorem 2. In §9, we give the values of b_n for $n \leq 44$, and the values of c_n for $n \leq 20$. In §10, we give an example with K an intermediate field between $\mathbb{Q}$ and $\mathbb{Q}(\lambda + \lambda^{-1})$.

2. Background

Every field K in this paper is a subfield of $\mathbb{C}$, and so every field K in this paper is perfect. This means that (1) all the roots of an irreducible polynomial with coefficients in K are simple, (2) every finite extension of K is separable, and (3) the algebraic closure $\overline{K}$ of K in $\mathbb{C}$ is the separable closure K_s of K.

Let R be a subring of $\mathbb{C}$. A polynomial $p(x)$ is *over R* if $p(x)$ has coefficients in R. A complex number α is an *algebraic integer* if α is the root of a monic polynomial over $\mathbb{Z}$. The set $\mathbb{A}$ of all algebraic integers is a subring of $\mathbb{C}$. The ring $\mathbb{A}$ is integrally closed in $\mathbb{C}$, that is, $\mathbb{A}$ contains the roots of every monic polynomial over $\mathbb{A}$, (cf. Exercise 4 on p. 39 of [21]).

Let α be an algebraic integer. A *minimal polynomial* of α over $\mathbb{Z}$ is a monic polynomial $p(x)$ over $\mathbb{Z}$ of lowest degree such that $p(\alpha) = 0$. A minimal polynomial $p(x)$ of α over $\mathbb{Z}$ is unique, since $p(x)$ is the minimal polynomial of α over $\mathbb{Q}$ by Theorem 1 of [21].

Let $p(x)$ be the minimal polynomial of α over $\mathbb{Z}$. The *degree* of α is the degree of $p(x)$. Each root of $p(x)$ is simple, since $p(x)$ is irreducible over $\mathbb{Q}$. The roots of $p(x)$ are called the *conjugates* of α. The conjugates of α are the algebraic integers with minimal polynomial $p(x)$ over $\mathbb{Z}$.

In this paper, a *Salem number* is a real algebraic integer $\lambda > 1$ such that λ^{-1} is a conjugate of λ and all remaining conjugates of λ are complex numbers of absolute value one. A Salem number is a unit of $\mathbb{A}$.

A *Salem polynomial* is the minimal polynomial over $\mathbb{Z}$ of a Salem number. Let $s(x)$ be the Salem polynomial of a Salem number λ. The units ± 1 are not roots of $s(x)$, since otherwise we could factor out $x \pm 1$ from $s(x)$. Hence the real roots of $s(x)$ are $\lambda^{\pm 1}$. The polynomial $s(x)$ is over $\mathbb{R}$, and so the complex roots of $s(x)$ pair off into pairs of complex numbers of the form $e^{\pm i\theta}$ for some real number θ with $0 < \theta < \pi$. Therefore $\deg \lambda$ is an even positive integer. We have that

$$(x - \lambda)(x - \lambda^{-1}) = x^2 - (\lambda + \lambda^{-1})x + 1,$$

with $\lambda + \lambda^{-1} > 2$. Hence $\deg \lambda = 2$ if and only if $\lambda + \lambda^{-1} \in \mathbb{Z}$.

The roots of $s(x)$ are simple and pair off into reciprocal pairs. Let $m = \deg s(x)$. Then $s(x) = x^m s(x^{-1})$. Hence if $s(x) = a_0 + \cdots + a_m x^m$, we have that $a_j = a_{m-j}$ for each j, that is, $s(x)$ is a palindromic polynomial.

Let f_n be the *Lorentzian quadratic form* in $n+1$ variables $x_1, \ldots, x_{n+1}$ given by

$$f_n(x) = x_1^2 + \cdots + x_n^2 - x_{n+1}^2.$$

The hyperboloid model of *hyperbolic n-space* is

$$H^n = \{x \in \mathbb{R}^{n+1} : f_n(x) = -1 \text{ and } x_{n+1} > 0\}.$$

The *orthogonal group* of the quadratic form f_n is defined to be

$$\mathrm{O}(n, 1) = \{T \in \mathrm{GL}(n + 1, \mathbb{R}) : f_n(Tx) = f_n(x) \text{ for all } x \in \mathbb{R}^{n+1}\}.$$

Let $\mathrm{O}'(n, 1)$ be the subgroup of $\mathrm{O}(n, 1)$ consisting of all $T \in \mathrm{O}(n, 1)$ that leave H^n invariant. Then $\mathrm{O}'(n, 1)$ has index 2 in $\mathrm{O}(n, 1)$, since $-I \in \mathrm{O}(n, 1)$ and $-I \notin \mathrm{O}'(n, 1)$, and if $T \in \mathrm{O}(n, 1)$ and $T \notin \mathrm{O}'(n, 1)$, then $-T \in \mathrm{O}'(n, 1)$. Restriction induces an isomorphism from $\mathrm{O}'(n, 1)$ to $\mathrm{Isom}(H^n)$. We will identify $\mathrm{O}'(n, 1)$ with the group of isometries of H^n.

Let R be a subring of $\mathbb{C}$. Let f be a nondegenerate quadratic form in $n + 1$ variables $x_1, \ldots, x_{n+1}$ with real coefficients $a_{ij} = a_{ji}$ for all i, j. We say that f is *over R* if $a_{ij} \in R$ for all i, j. The *orthogonal group* of f over R is defined to be

$$\mathrm{O}(f, R) = \{T \in \mathrm{GL}(n + 1, R) : f(Tx) = f(x) \text{ for all } x \in \mathbb{R}^{n+1}\}.$$

Let $A = (a_{ij})$ be the coefficient matrix of the quadratic form f. Then A is an $(n + 1) \times (n + 1)$ symmetric matrix over $\mathbb{R}$ and $f(x) = x^t A x$ for all $x \in \mathbb{R}^{n+1}$. We have that

$$\mathrm{O}(f, R) = \{T \in \mathrm{GL}(n + 1, R) : T^t A T = A\}.$$

Suppose that the quadratic form f has signature $(n, 1)$. This means that there exists $M \in \mathrm{GL}(n+1, \mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$. Then M maps the set $\{x \in \mathbb{R}^{n+1} : f_n(x) < 0\}$ onto the set $\{x \in \mathbb{R}^{n+1} : f(x) < 0\}$. Hence the set $\{x \in \mathbb{R}^{n+1} : f(x) < 0\}$ is a cone with two connected components.

If R is a subring of $\mathbb{R}$, let $\mathrm{O}'(f, R)$ be the subgroup of $\mathrm{O}(f, R)$ consisting of all $T \in \mathrm{O}(f, R)$ that leave both components of the cone $\{x \in \mathbb{R}^{n+1} : f(x) < 0\}$

invariant. Then $\mathrm{O}'(f,R)$ has index 2 in $\mathrm{O}(f,R)$, since $-I \in \mathrm{O}(f,R)$ and $-I \notin \mathrm{O}'(f,R)$, and if $T \in \mathrm{O}(f,R)$ and $T \notin \mathrm{O}'(f,R)$, then $-T \in \mathrm{O}'(f,R)$. We have that

$$M\mathrm{O}'(n,1)M^{-1} = \mathrm{O}'(f,\mathbb{R}).$$

Let K be a totally real number field and subfield of $\mathbb{R}$, and let $\mathfrak{o}_K$ be the ring of all algebraic integers in K. Let f be a quadratic form over K in $n+1$ variables with coefficient matrix $A = (a_{ij})$. The quadratic form f is said to be *admissible* if f has signature $(n,1)$, and for each nonidentity embedding $\sigma : K \to \mathbb{R}$ the quadratic form f^σ over $\sigma(K)$, with coefficient matrix $A^\sigma = (\sigma(a_{ij}))$, is positive definite.

A subgroup Γ of $\mathrm{O}'(n,1)$ is an *arithmetic group of isometries of H^n of the simplest type defined over K* if there exists an admissible quadratic form f over K in $n+1$ variables, and there exists $M \in \mathrm{GL}(n+1,\mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, and $M\Gamma M^{-1}$ is commensurable to $\mathrm{O}'(f,\mathfrak{o}_K)$ in $\mathrm{O}'(f,\mathbb{R})$, that is, $M\Gamma M^{-1} \cap \mathrm{O}'(f,\mathfrak{o}_K)$ has finite index in both $M\Gamma M^{-1}$ and $\mathrm{O}'(f,\mathfrak{o}_K)$.

A subgroup Γ of $\mathrm{O}'(n,1)$ is a *classical arithmetic group of isometries of H^n of the simplest type defined over K* if there exists an admissible quadratic form f over K in $n+1$ variables, and there exists $M \in \mathrm{GL}(n+1,\mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, and $M\Gamma M^{-1} \subseteq \mathrm{O}'(f,K)$ with $M\Gamma M^{-1}$ commensurable to $\mathrm{O}'(f,\mathfrak{o}_K)$.

Let Γ be an arithmetic group of isometries of H^n of the simplest type defined over K with respect to an admissible quadratic form f. Then Γ is a discrete subgroup of $\mathrm{O}'(n,1)$, (cf. §12 of [8]). The hyperbolic orbifold H^n/Γ is compact unless $K = \mathbb{Q}$ and there exists $x \neq 0$ in $\mathbb{Q}^{n+1}$ such that $f(x) = 0$ (cf. §12 of [8]). Suppose that $K = \mathbb{Q}$. If $n = 1,2,3$, then H^n/Γ is compact for some f and not compact for some f. If $n > 3$, then H^n/Γ is not compact, since there exists $x \neq 0$ in $\mathbb{Q}^{n+1}$ such that $f(x) = 0$ (cf. [10] p 75). If $n > 1$, then H^n/Γ has finite volume [8].

3. Preliminary Algebraic Lemmas

The point of departure of our work in this paper is our first lemma, which was motivated by Takeuchi's lemma [29].

Lemma 1. *Let K be a subfield of $\mathbb{C}$, and let $\mathfrak{o}_K$ be the ring of algebraic integers of K. Let A be an $n \times n$ matrix over K such that A^m is over $\mathfrak{o}_K$ for some positive integer m. Then the characteristic polynomial* $\mathrm{char}(A)$ *of A is over $\mathfrak{o}_K$.*

Proof. We have that $\mathrm{char}(A^m)$ is a monic polynomial over $\mathfrak{o}_K$. Hence the roots of $\mathrm{char}(A^m)$ are in $\mathbb{A}$, since $\mathbb{A}$ is integrally closed in $\mathbb{C}$. The roots of $\mathrm{char}(A^m)$ are the mth powers of the roots of $\mathrm{char}(A)$. Hence the roots $r_1, \ldots, r_n$ of $\mathrm{char}(A)$ are mth roots of the roots of $\mathrm{char}(A^m)$. Therefore $r_i \in \mathbb{A}$ for each i, since $\mathbb{A}$ is integrally closed in $\mathbb{C}$. Now we have

$$\mathrm{char}(A)(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$$

and so $\mathrm{char}(A)$ is over $\mathbb{A} \cap K = \mathfrak{o}_K$. □

Let R be a subring of $\mathbb{C}$. A polynomial $p(x)$ over R is said to be *irreducible over R* if whenever $p(x) = f(x)g(x)$ with $f(x)$ and $g(x)$ over R, then either $f(x)$ or $g(x)$ is a unit in R. The next lemma is elementary.

Lemma 2. *Let R be a subring of $\mathbb{C}$. A monic polynomial $p(x)$ over R is irreducible over R if and only if whenever $p(x) = f_1(x)g_1(x)$ with $f_1(x)$ and $g_1(x)$ monic polynomials over R, then either $f_1(x) = 1$ or $g_1(x) = 1$.*

The next lemma generalizes Gauss's lemma for monic polynomials over $\mathbb{Z}$.

Lemma 3. *Let K be a subfield of $\mathbb{C}$, and let $\mathfrak{o}_K$ be the ring of algebraic integers of K. Let $p(x)$ be an irreducible monic polynomial over $\mathfrak{o}_K$. Then $p(x)$ is irreducible over K.*

Proof. Suppose $p(x) = f(x)g(x)$ with $f(x)$ and $g(x)$ monic polynomials over K. The roots of $f(x)$ together with the roots of $g(x)$ are the roots of $p(x)$. The roots of $p(x)$ are in $\mathbb{A}$, since $\mathbb{A}$ is integrally closed in $\mathbb{C}$. Hence the roots of $f(x)$ and $g(x)$ are in $\mathbb{A}$. Therefore $f(x)$ and $g(x)$ are over $\mathbb{A} \cap K = \mathfrak{o}_K$. As $p(x)$ is irreducible over $\mathfrak{o}_K$, we have that either $f(x) = 1$ or $g(x) = 1$ by Lemma 2. Hence $p(x)$ is irreducible over K by Lemma 2. □

The next lemma generalizes a well known lemma for Salem polynomials.

Lemma 4. *Let K be a subfield of $\mathbb{R}$, and let $\mathfrak{o}_K$ be the ring of algebraic integers of K. Let $p(x)$ be an irreducible monic polynomial over $\mathfrak{o}_K$ of degree $m = 2\ell$ whose real roots are λ and λ^{-1}, with $\lambda > 1$, and whose complex roots have absolute value equal to 1. Then there exists a unique monic irreducible polynomial $q(x)$ over $\mathfrak{o}_K$ of degree ℓ, called the trace polynomial of $p(x)$, such that $p(x) = x^\ell q(x + x^{-1})$.*

Proof. The polynomial $p(x)$ is irreducible over K by Lemma 3. Hence all the roots of $p(x)$ are simple. The polynomial $p(x)$ is over $\mathbb{R}$, and so the complex roots of $p(x)$ pair off into pairs of the form $e^{\pm i\theta}$ for some real number θ. Hence the roots of $p(x)$ are $r_1, r_1^{-1}, \ldots, r_\ell, r_\ell^{-1}$ with $r_1 = \lambda$, and if $j > 1$, then $r_j = e^{i\theta_j}$ with $0 < \theta_j < \pi$, and if $1 < j < k \leq \ell$, then $\theta_j < \theta_k$.

Now we have that $r_1 + r_1^{-1} = \lambda + \lambda^{-1} > 2$, and if $j > 1$, then $r_j + r_j^{-1} = 2\cos\theta_j$. Hence $r_1 + r_1^{-1}, \ldots, r_\ell + r_\ell^{-1}$ is a strictly decreasing sequence of real numbers.

The equation

$$p(x) = x^\ell q(x + x^{-1})$$

implies that $q(x)$ must be monic and the roots of $q(x)$ must be $r_1+r_1^{-1}, \ldots, r_\ell+r_\ell^{-1}$. Hence $q(x)$ must be defined by the equation

$$q(x) = \big(x - (r_1 + r_1^{-1})\big) \cdots \big(x - (r_\ell + r_\ell^{-1})\big).$$

Observe that

$$\begin{aligned} x^\ell q(x + x^{-1}) &= x^\ell\big((x + x^{-1} - (r_1 + r_1^{-1})) \cdots (x + x^{-1} - (r_\ell + r_\ell^{-1}))\big) \\ &= \big(x^2 - (r_1 + r_1^{-1})x + 1\big) \cdots \big(x^2 - (r_\ell + r_\ell^{-1})x + 1\big) \\ &= (x - r_1)(x - r_1^{-1}) \cdots (x - r_\ell)(x - r_\ell^{-1}) \quad = \quad p(x). \end{aligned}$$

Hence $q(x)$ is the unique polynomial over $\mathbb{R}$ such that $p(x) = x^\ell q(x + x^{-1})$.

Let a_j be the jth degree coefficient of $p(x)$. The monic polynomials $p(x)$ and $x^m p(x^{-1})$ have the same roots, and so $p(x) = x^m p(x^{-1})$. Hence $p(x)$ is palindromic, that is, $a_j = a_{m-j}$ for all j. Therefore $p(x)$ is determined by $a_0, \ldots, a_\ell$.

Let b_j be the jth degree coefficient of $q(x)$. The equation $p(x) = x^\ell q(x + x^{-1})$ implies that each a_j can be written as a linear combination of $b_0, \ldots, b_\ell$ over $\mathbb{Z}$. Hence there is an $(\ell + 1) \times (\ell + 1)$ matrix M over $\mathbb{Z}$ such that

$$M(b_0, \ldots, b_\ell)^t = (a_0, \ldots, a_\ell)^t.$$

As $(b_0, \ldots, b_\ell)$ is the unique solution of the inhomogeneous linear system

$$M(x_0, \ldots, x_\ell)^t = (a_0, \ldots, a_\ell)^t,$$

the matrix M is invertible, and so

$$(b_0, \dots, b_\ell)^t = M^{-1}(a_0, \dots, a_\ell)^t.$$

Therefore $b_j \in K$ for each j.

The roots of $p(x)$ are in $\mathbb{A}$, since $\mathbb{A}$ is integrally closed in $\mathbb{C}$. Hence the roots of $q(x)$ are in $\mathbb{A}$. Therefore $q(x)$ is over $\mathbb{A} \cap K = \mathfrak{o}_K$.

Suppose $q(x) = f(x)g(x)$ with $f(x)$ and $g(x)$ monic polynomials over $\mathfrak{o}_K$. Let $j = \deg(f)$ and $k = \deg(g)$. Then $j + k = \ell$ and

$$p(x) = x^\ell q(x + x^{-1}) = \big(x^j f(x + x^{-1})\big)\big(x^k g(x + x^{-1})\big).$$

The polynomials $x^j f(x + x^{-1})$ and $x^k g(x + x^{-1})$ are monic. Hence we have either $x^j f(x + x^{-1}) = 1$ or $x^k g(x + x^{-1}) = 1$, since $p(x)$ is irreducible over $\mathfrak{o}_K$. Therefore either $f(x) = 1$ or $g(x) = 1$, and so $q(x)$ is irreducible over $\mathfrak{o}_K$ by Lemma 2. □

The next lemma was communicated to us by David Boyd.

Lemma 5. *Let K be a number field. Then K is totally real if and only if there is a Salem number λ such that $K = \mathbb{Q}(\lambda + \lambda^{-1})$.*

Proof. Suppose λ is a Salem number and $K = \mathbb{Q}(\lambda + \lambda^{-1})$. Let $p(x)$ be the Salem polynomial for λ of degree 2ℓ. By Lemma 4, there is an irreducible polynomial $q(x)$ over $\mathbb{Z}$ such that $p(x) = x^\ell q(x + x^{-1})$. The polynomial $q(x)$ is irreducible over $\mathbb{Q}$ by Lemma 3. Hence $q(x)$ is the minimal polynomial of $\lambda + \lambda^{-1}$ over $\mathbb{Q}$. Moreover all the roots of $q(x)$ are real by the proof of Lemma 4. If $\sigma : K \to \mathbb{C}$ is an embedding, then there exists a root β of $q(x)$ so that $\sigma(\lambda + \lambda^{-1}) = \beta$ (cf. [17] p 171). Hence K is totally real.

Conversely, suppose K is totally real. Then there exists a Pisot number α such that $K = \mathbb{Q}(\alpha)$ by Hilfssatz 1 of [25] or Theorem 5.2.2 of [4]. Now α is a real algebraic integer with $\alpha > 1$. Let $f(x)$ be the minimal polynomial of α over $\mathbb{Z}$. Then all the roots of $f(x)$ besides α have absolute value less than 1. As K is totally real, all the roots of $f(x)$ are real. Let $\ell = \deg f(x)$. Then 2α is an algebraic integer with minimal polynomial $g(x) = 2^\ell f(x/2)$ over $\mathbb{Z}$ all of whose roots besides 2α lie in the interval $(-2, 2)$. Let λ be the solution of $x + x^{-1} = 2\alpha$ that is greater than one. Then $h(x) = x^\ell g(x + x^{-1})$ is a Salem polynomial with Salem number λ. We have that $K = \mathbb{Q}(2\alpha) = \mathbb{Q}(\lambda + \lambda^{-1})$. □

Let K be a totally real number field and subfield of $\mathbb{R}$. We now give an example of a classical arithmetic group of isometries of H^n of the simplest type defined over K. By Lemma 5, there is a Salem number λ such that $K = \mathbb{Q}(\lambda + \lambda^{-1})$. We have that $\lambda + \lambda^{-1} > 2$. Therefore the quadratic form

$$f(x) = x_1^2 + \cdots + x_n^2 - (\lambda + \lambda^{-1} - 2)x_{n+1}^2$$

is over K and has signature $(n, 1)$. Let $\sigma : K \to \mathbb{R}$ be a nonidentity embedding. Then $\sigma(\lambda + \lambda^{-1}) = 2\cos\theta$ for some real number θ such that $0 < \theta < \pi$ by the proof of Lemma 4. Therefore f^σ is positive definite. Thus f is admissible.

Let M be the diagonal $(n+1) \times (n+1)$ matrix

$$M = \mathrm{diag}(1, \dots, 1, (\lambda + \lambda^{-1} - 2)^{-1/2}).$$

Then we have that $f(Mx) = f_n(x)$. Hence $\Gamma = M^{-1}\mathrm{O}'(f, \mathfrak{o}_K)M$ is a classical arithmetic group of isometries of H^n of the simplest type defined over K.

4. Linear Algebraic Group Lemmas

In this section, we prove some lemmas that require the theory of linear algebraic groups [5]. Let f be a quadratic form over a subfield K of $\mathbb{R}$ of signature $(n, 1)$. We are primarily interested in algebraic K-subgroups of $\mathrm{GL}(n+1, \mathbb{C})$ such as $\mathrm{O}(f, \mathbb{C})$ with the exception of the quotient algebraic K-group $\mathrm{PO}(f, \mathbb{C}) = \mathrm{O}(f, \mathbb{C})/\{\pm I\}$ whose algebraic K-group structure is described in matrix terms in Lemma 7 below.

Recall that a subgroup Γ of $\mathrm{O}'(n, 1)$ is a (classical) arithmetic group of isometries of H^n of the simplest type defined over a totally real number field K if there exists an admissible quadratic form f over K in $n+1$ variables, and there exists $M \in \mathrm{GL}(n+1, \mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, $\big($and $M\Gamma M^{-1} \subseteq \mathrm{O}'(f, K)\big)$, with $M\Gamma M^{-1}$ commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$ in $\mathrm{O}'(f, \mathbb{R})$.

Let H be a subgroup of a group G. The *commensurator* of H in G is the group

$$C(H) = \{g \in G : H \text{ is commensurable to } gHg^{-1}\}.$$

If H and H' are commensurable subgroups of G, then $C(H) = C(H')$, since commensurability is an equivalence relation on the set of subgroups of G. If $\phi : G \to G'$ is a homomorphism of groups, then $\phi(C(H)) \subseteq C(\phi(H))$.

Lemma 6. *Let Γ be an arithmetic group of isometries of H^n, with n even, of the simplest type defined over K, then Γ is a classical arithmetic group of isometries of H^n of the simplest type defined over K.*

Proof. There exists an admissible quadratic form f over K in $n+1$ variables and there exists $M \in \mathrm{GL}(n+1, \mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, and $M\Gamma M^{-1}$ is commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$ in $\mathrm{O}'(f, \mathbb{R})$. Define $\psi : \mathrm{O}'(f, \mathbb{R}) \to \mathrm{SO}(f, \mathbb{R})$ by $\psi(A) = (\det A)A$. Then ψ is an isomorphism, since ψ restricts to the identity map on $\mathrm{SO}'(f, \mathbb{R}) = \mathrm{O}'(f, \mathbb{R}) \cap \mathrm{SO}(f, \mathbb{R})$ and $\mathrm{SO}'(f, \mathbb{R})$ has index 2 in both $\mathrm{O}'(f, \mathbb{R})$ and $\mathrm{SO}(f, \mathbb{R})$. Let $\overline{\Gamma} = \psi(M\Gamma M^{-1})$. Then $\overline{\Gamma}$ is commensurable to $\Lambda = \mathrm{SO}(f, \mathfrak{o}_K)$, since $\psi(\mathrm{O}'(f, \mathfrak{o}_K)) = \Lambda$.

The group $G = \mathrm{SO}(f, \mathbb{C})$ is a connected algebraic K-group for all even $n \geq 2$. We have that $[\mathrm{O}(f, \mathbb{C}), \mathrm{O}(f, \mathbb{C})] = [G, G]$ by Theorem 3.23 of [2], and so $G = [G, G]$ by Theorem 5.18 of [2]. Hence the character group $X(G)$ of G is trivial (cf. §2.2 of [5]). The group $G_{\mathbb{R}} = \mathrm{SO}(f, \mathbb{R})$ is not compact, since f has signature $(n, 1)$. For each nonidentity field embedding $\sigma : K \to \mathbb{R}$, the group $G^\sigma_{\mathbb{R}} = \mathrm{SO}(f^\sigma, \mathbb{R})$ is compact, since f^σ is positive definite. Therefore Λ is a discrete subgroup of $G_{\mathbb{R}}$ such that $G_{\mathbb{R}}/\Lambda$ has finite Haar measure by Theorem 12.3 of [8]. Hence Λ is infinite, since $G_{\mathbb{R}}$ has infinite Haar measure.

The group of K-points of G is $G_K = \mathrm{SO}(f, K)$. Let $C(\Lambda)$ be the commensurator of Λ in G. We claim that $G_K \subseteq C(\Lambda)$. Let $C \in G_K$. Then there exists a positive integer m such that mC and mC^{-1} are over $\mathfrak{o}_K$. Let Λ_m be the congruence m^2 subgroup of Λ. Let $A \in \Lambda_m$. Then $A = I + m^2B$ with B over $\mathfrak{o}_K$. Now $CAC^{-1} = I + m^2CBC^{-1}$ is over $\mathfrak{o}_K$. Hence $C\Lambda_mC^{-1} \subseteq \Lambda$, and so $\Lambda_m \subseteq C^{-1}\Lambda C$. Likewise $C^{-1}\Lambda_mC \subseteq \Lambda$, and so $\Lambda_m \subseteq C\Lambda C^{-1}$. Therefore $\Lambda_m \subseteq \Lambda \cap C\Lambda C^{-1}$ and $\Lambda_m \subseteq \Lambda \cap C^{-1}\Lambda C$, and so $\Lambda \cap C\Lambda C^{-1}$ and $\Lambda \cap C^{-1}\Lambda C$ are of finite index in Λ. Applying conjugation by C to $\Lambda \cap C^{-1}\Lambda C$ gives that $C\Lambda C^{-1} \cap \Lambda$ is of finite index in $C\Lambda C^{-1}$. Hence $C \in C(\Lambda)$. Therefore $G_K \subseteq C(\Lambda)$.

The center of G is trivial by Theorem 3.23 of [2], and so G is isomorphic to its adjoint group (cf. §3.15 of [7]). The group G is simple by Theorems 5.20 and 5.27 of [2]. The group G_K is Zariski-dense in G by (3) in §5.4 of [5]. Hence $C(\Lambda)$

is Zariski-dense in G, since $G_K \subseteq C(\Lambda)$. Therefore Λ is Zariski-dense in G and $C(\Lambda) \subseteq G_K$ by the K-version of Lemma 15.11 of [6] (cf. Remarks on p 106 of [6]). As $\overline{\Gamma}$ is commensurable to Λ in G, we have that

$$\overline{\Gamma} \subseteq C(\overline{\Gamma}) = C(\Lambda) = G_K.$$

As $\psi(\mathrm{O}'(f,K)) = G_K$, we have that $M\Gamma M^{-1} \subseteq \mathrm{O}'(f,K)$. Therefore Γ is a classical arithmetic group of isometries of H^n of the simplest type defined over K. □

Let f be a nondegenerate quadratic form in $n+1$ variables over a subfield K of $\mathbb{R}$ with n odd, and let A be the coefficient matrix of f. The *general orthogonal group* of f (cf. [15] p 154) is the group

$$\mathrm{GO}(f) = \{B \in \mathrm{GL}(n+1,\mathbb{C}) : B^tAB = bA \text{ for some } b \in \mathbb{C}\}.$$

If $B \in \mathrm{GO}(f)$ and $B^tAB = bA$ with $b \in \mathbb{C}$, then $bI = B^tABA^{-1}$, and so $b \neq 0$ and b is uniquely determined by B. We write $\mu(B)$ for b. If $c \in \mathbb{C}^*$, then $cI \in \mathrm{GO}(f)$ and $\mu(cI) = c^2$. Hence, the map $\mu : \mathrm{GO}(f) \to \mathbb{C}^*$ is an epimorphism with kernel equal to $\mathrm{O}(f)$.

If $B \in \mathrm{GO}(f)$ and $b = \mu(B)$, then $(\det B)^2 = b^{n+1}$, and so $\det B = \pm b^{(n+1)/2}$. The *general special orthogonal group* of f (cf. [15] p 154) is the group

$$\mathrm{GSO}(f) = \{B \in \mathrm{GO}(f) : \det B = b^{(n+1)/2} \text{ with } b = \mu(B)\}.$$

Let $D = \{cI_{n+1} : c \in \mathbb{C}^*\}$. Then D is a normal subgroup of $\mathrm{GO}(f)$. The *projective general orthogonal group* of f is the group $\mathrm{PGO}(f) = \mathrm{GO}(f)/D$.

Let $\mathrm{GO}(f,K) = \mathrm{GO}(f) \cap \mathrm{GL}(n+1,K)$. Suppose $B \in \mathrm{GO}(f,K)$. Then $B^tAB = bA$ with $b = \mu(B)$. Hence $b \in K^*$. Now B represents an equivalence from f to bf over K, and so f and bf have the same signature (p,q). If $p \neq q$, we must have $b > 0$. If f is an admissible quadratic form over a totally real number field K and $n \geq 3$, then we have that $\sigma(b) > 0$ for each field embedding $\sigma : K \to \mathbb{R}$, that is, b is *totally positive* (cf. [11] p 401).

Lemma 7. *Let f be a quadratic form in $n+1$ variables over a subfield K of $\mathbb{R}$ of signature $(n,1)$ with n odd and $n \geq 3$. Let $\mathrm{PO}(f)$ be the algebraic K-group $\mathrm{O}(f,\mathbb{C})/\{\pm I\}$, and let $\mathrm{PO}(f)_K$ be the group of K-points of $\mathrm{PO}(f)$. Then*

$$\mathrm{PO}(f)_K = \{\{\pm\tfrac{1}{\sqrt{b}}B\} : B \in \mathrm{GO}(f,K) \text{ and } b = \mu(B)\}.$$

Proof. Let $\pi : \mathrm{O}(f) \to \mathrm{PO}(f)$ and $\eta : \mathrm{GO}(f) \to \mathrm{PGO}(f)$ be the quotient maps. Then π and η are K-homomorphisms of algebraic K-groups by Theorem 6.8 of [7]. The inclusion map $\upsilon : \mathrm{O}(f) \to \mathrm{GO}(f)$ is a K-homomorphism. By the Universal Mapping Property ([7] p 94), the inclusion $\upsilon : \mathrm{O}(f) \to \mathrm{GO}(f)$ induces a K-homomorphism $\overline{\upsilon} : \mathrm{PO}(f) \to \mathrm{PGO}(f)$ such that $\overline{\upsilon}\pi = \eta\upsilon$. If $B \in \mathrm{O}(f)$, then $\overline{\upsilon}(\{\pm B\}) = DB$, and so $\overline{\upsilon}$ is a monomorphism. Now assume that $B \in \mathrm{GO}(f)$, and let $b = \mu(B)$. Then $\det B = \pm b^{(n+1)/2}$. Hence $\det(\frac{1}{\sqrt{b}}B) = \pm 1$. We have that $\overline{\upsilon}(\{\pm\frac{1}{\sqrt{b}}B\}) = DB$, and so $\overline{\upsilon}$ is onto, and therefore $\overline{\upsilon}$ is a group isomorphism.

Let $\overline{K}$ be the algebraic closure of K in $\mathbb{C}$. Then π maps $\mathrm{O}(f)_{\overline{K}} = \mathrm{O}(f,\overline{K})$ onto $\mathrm{PO}(f)_{\overline{K}}$ and η maps $\mathrm{GO}(f)_{\overline{K}} = \mathrm{GO}(f,\overline{K})$ onto $\mathrm{PGO}(f)_{\overline{K}}$ (cf. [7] p 99). As $\upsilon : \mathrm{O}(f) \to \mathrm{GO}(f)$ is a K-homomorphism, $\upsilon(\mathrm{O}(f,\overline{K})) \subseteq \mathrm{GO}(f,\overline{K})$. Therefore $\overline{\upsilon}(\mathrm{PO}(f)_{\overline{K}}) \subseteq \mathrm{PGO}(f)_{\overline{K}}$. Let $B \in \mathrm{GO}(f,\overline{K})$ and let $b = \mu(B)$, then $b \in \overline{K}$, and so $\sqrt{b} \in \overline{K}$. Hence $\frac{1}{\sqrt{b}}B \in \mathrm{O}(f,\overline{K})$. Therefore $\{\pm\frac{1}{\sqrt{b}}B\} \in \mathrm{PO}(f)_{\overline{K}}$ and $\overline{\upsilon}(\{\pm\frac{1}{\sqrt{b}}B\}) = DB$. Hence $\overline{\upsilon}(\mathrm{PO}(f)_{\overline{K}}) = \mathrm{PGO}(f)_{\overline{K}}$.

The Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $\mathrm{O}(f,\overline{K})$ and $\mathrm{GO}(f,\overline{K})$ coordinate-wise, and acts on $\mathrm{PO}(f)_{\overline{K}}$ and $\mathrm{PGO}(f)_{\overline{K}}$ so that the quotient maps $\pi : \mathrm{O}(f) \to \mathrm{PO}(f)$ and $\eta : \mathrm{GO}(f) \to \mathrm{PGO}(f)$ commute with the action of $\mathrm{Gal}(\overline{K}/K)$ (cf. [7] p 31). As $\overline{v}$ is a K-homomorphism, $\overline{v}$ commutes with the actions of $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{PO}(f)_{\overline{K}}$ and $\mathrm{PGO}(f)_{\overline{K}}$ (cf. [7] p 31).

The group $\mathrm{PO}(f)_K$ is the subgroup of $\mathrm{PO}(f)_{\overline{K}}$ of elements fixed by $\mathrm{Gal}(\overline{K}/K)$, and $\mathrm{PGO}(f)_K$ is the subgroup of $\mathrm{PGO}(f)_{\overline{K}}$ of elements fixed by $\mathrm{Gal}(\overline{K}/K)$ (cf. §AG.14 of [7]). Therefore $\overline{v}$ restricts to an isomorphism $\overline{v}_* : \mathrm{PO}(f)_K \to \mathrm{PGO}(f)_K$.

Let $\zeta : D \to \mathrm{GO}(f)$ be the inclusion. Then ζ is a K-homomorphism. The short exact sequence of algebraic K-groups and K-homomorphisms

$$1 \to D \xrightarrow{\zeta} \mathrm{GO}(f) \xrightarrow{\eta} \mathrm{PGO}(f) \to 1$$

determines an exact sequence of Galois cohomology groups and homomorphisms

$$1 \to D_K \xrightarrow{\zeta_*} \mathrm{GO}(f)_K \xrightarrow{\eta_*} \mathrm{PGO}(f)_K \xrightarrow{\delta} H^1(K,D)$$

with ζ_* a restriction of ζ and η_* a restriction of η by the discussion in §1.3 of [9] and Proposition 1.17 and Corollary 1.23 of [9]. The algebraic K-group D is K-isomorphic to the cartesian product $(\mathbb{C}^*)^{n+1}$, and so $H^1(K,D) = 0$ by Proposition 1 on p 72 of [27] and induction on n. Hence $\eta_*(\mathrm{GO}(f)_K) = \mathrm{PGO}(f)_K$. We have that $\mathrm{GO}(f)_K = \mathrm{GO}(f,K)$, and so

$$\mathrm{PGO}(f)_K = \{DB : B \in \mathrm{GO}(f,K)\}.$$

Therefore

$$\mathrm{PO}(f)_K = \overline{v}_*^{-1}(\mathrm{PGO}(f)_K) = \{\{\pm\tfrac{1}{\sqrt{b}}B\} : B \in \mathrm{GO}(f,K) \text{ and } b = \mu(B)\}. \qquad \square$$

Lemma 8. *Let f be a quadratic form in $n+1$ variables over $\mathbb{R}$ of signature $(n,1)$ with n odd and $n \geq 3$. Then the algebraic $\mathbb{R}$-group $\mathrm{PSO}(f) = \mathrm{SO}(f,\mathbb{C})/\{\pm I\}$ is $\mathbb{R}$-simple (no nontrivial proper normal $\mathbb{R}$-subgroups).*

Proof. Let $\mathrm{O}(f) = \mathrm{O}(f,\mathbb{C})$ and $\mathrm{SO}(f) = \mathrm{SO}(f,\mathbb{C})$. We have that $[\mathrm{O}(f),\mathrm{O}(f)] = [\mathrm{SO}(f),\mathrm{SO}(f)]$ by Theorem 3.23 of [2], and $\mathrm{SO}(f) = [\mathrm{O}(f),\mathrm{O}(f)]$ by Theorem 5.18 of [2]. Hence $\{\pm I\}$ is the center of $\mathrm{SO}(f)$ by Theorem 3.23 of [2]. Therefore $\mathrm{PSO}(f)$ is a simple group for all odd $n \geq 5$ by Theorem 5.27 of [2]. Hence we may assume that $n = 3$.

We have that $\mathrm{PSO}(f)$ is $\mathbb{C}$-isomorphic to $\mathrm{PSL}(2,\mathbb{C}) \times \mathrm{PSL}(2,\mathbb{C})$ by Theorem 5.22 of [2]. The group $H = \mathrm{PSL}(2,\mathbb{C})$ is simple by Theorem 4.10 of [2]. Moreover H is nonabelian. Let N be a nontrivial proper normal $\mathbb{R}$-subgroup of $\mathrm{PSO}(f)$. Then N corresponds to a nontrivial proper normal subgroup M of $H \times H$. We claim that $M = H \times 1$ or $M = 1 \times H$.

Let $\pi_2 : H \times H \to H$ be the projection onto the second factor. Then $\pi_2(M) \lhd H$ and so $\pi_2(M) = 1$ or H. If $\pi_2(M) = 1$, then $M \lhd (H \times 1)$, and so $M = H \times 1$. Hence we may assume that $\pi_2(M) = H$. Now $M \cap (H \times 1) \lhd (H \times 1)$. Hence $M \cap (H \times 1) = 1$ or $H \times 1$. If $M \cap (H \times 1) = H \times 1$, then $H \times 1 \subseteq M$, and so $M = H \times H$, which is not the case. Hence $M \cap (H \times 1) = 1$. Suppose $(h_1,h),(h_2,h) \in M$. Then $(h_1h_2^{-1},1) \in M$, and so $h_1 = h_2$. If $h \in H$ and $(h_1,h_2) \in M$, then $(hh_1h^{-1},h_2) \in M$, and so $hh_1h^{-1} = h_1$. Hence $h_1 \in Z(H) = 1$. Therefore $M = 1 \times H$.

Hence N is $\mathbb{C}$-isomorphic to $\mathrm{PSL}(2,\mathbb{C})$. The group $N_{\mathbb{R}}$ of real points of N is a normal subgroup of $\mathrm{PSO}(f)_{\mathbb{R}}$. We have that $\mathrm{PSO}(f)_{\mathbb{R}} = \mathrm{PSO}(f,\mathbb{R})$ by Lemma 7. The group $\mathrm{SO}'(f,\mathbb{R}) = \mathrm{O}'(f,\mathbb{R}) \cap \mathrm{SO}(f)$ is the kernel of the spinorial norm map from $\mathrm{SO}(f,\mathbb{R})$ to $\mathbb{R}^*/\mathbb{R}^{*2}$. Hence $\mathrm{SO}'(f,\mathbb{R})$ is isomorphic to $\mathrm{PSL}(2,\mathbb{C})$ by Theorem 5.21 of [2]. Define $\psi : \mathrm{SO}'(f,\mathbb{R}) \to \mathrm{PSO}(f,\mathbb{R})$ by $\psi(A) = \{\pm A\}$. Then ψ is an isomorphism, since $\mathrm{SO}'(f,\mathbb{R})$ has index 2 in $\mathrm{SO}(f,\mathbb{R})$ and $-I \notin \mathrm{SO}'(f,\mathbb{R})$. Therefore $\mathrm{PSO}(f,\mathbb{R})$ is isomorphic to $\mathrm{PSL}(2,\mathbb{C})$. As $\mathrm{PSL}(2,\mathbb{C})$ is a simple group, $N_{\mathbb{R}} = 1$ or $\mathrm{PSO}(f,\mathbb{R})$.

Let $\mathfrak{N}$ and $\mathfrak{N}_{\mathbb{R}}$ be the Lie algebras of N and $N_{\mathbb{R}}$ over $\mathbb{C}$ and $\mathbb{R}$ respectively. Then $\mathfrak{N} = \mathfrak{N}_{\mathbb{R}} \otimes \mathbb{C}$ (cf. [8] p 498). Hence $\dim_{\mathbb{R}}(N_{\mathbb{R}}) = \dim_{\mathbb{C}}(N) = 3$. As $\dim_{\mathbb{R}}(\mathrm{PSO}(f,\mathbb{R})) = 6$, we have a contradiction. Thus $\mathrm{PSO}(f)$ is $\mathbb{R}$-simple. □

Lemma 9. *Let Γ be an arithmetic group of isometries of H^n of the simplest type defined over K with respect to an admissible quadratic form f, with n odd and $n \geq 3$, and let $M \in \mathrm{GL}(n+1,\mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$ and $\Gamma' = M\Gamma M^{-1}$ is commensurable to $\mathrm{O}'(f,\mathfrak{o}_K)$ in $\mathrm{O}'(f,\mathbb{R})$. Let $\overline{\Gamma}$ be the image of Γ' in $\mathrm{PO}(f,\mathbb{R})$, and let $\mathrm{PO}(f)_K$ be the group of K-points of the algebraic K-group $\mathrm{PO}(f) = \mathrm{O}(f,\mathbb{C})/\{\pm I\}$. Then $\overline{\Gamma} \subseteq \mathrm{PO}(f)_K$.*

Proof. Let $G = \mathrm{SO}(f,\mathbb{C})$ and $\overline{G} = \mathrm{PSO}(f,\mathbb{C})$. Then G and $\overline{G}$ are a connected algebraic K-group for all odd $n \geq 3$. Let $\Lambda = \mathrm{SO}(f,\mathfrak{o}_K)$. Then Λ is infinite by the same argument as in the proof of Lemma 6. Hence $\overline{\Lambda} = \mathrm{PSO}(f,\mathfrak{o}_K)$ is infinite.

Define $\psi : \mathrm{O}'(f,\mathbb{R}) \to \mathrm{PO}(f,\mathbb{R})$ by $\psi(A) = \{\pm A\}$. Then ψ is an isomorphism, since $-I \notin \mathrm{O}'(f,\mathbb{R})$ and $\mathrm{O}'(f,\mathbb{R})$ has index 2 in $\mathrm{O}(f,\mathbb{R})$. Hence $\psi(\Gamma') = \overline{\Gamma}$ is commensurable to $\psi(\mathrm{O}'(f,\mathfrak{o}_K)) = \mathrm{PO}(f,\mathfrak{o}_K)$. Let $\overline{\Gamma}_0 = \overline{\Gamma} \cap \overline{G}$. Then $\overline{\Gamma}_0$ is commensurable to $\overline{\Lambda}$, since $\overline{\Gamma}_0$ has index at most 2 in $\overline{\Gamma}$ and $\overline{\Lambda}$ has index at most 2 in $\mathrm{PO}(f,\mathfrak{o}_K)$.

By Lemma 7, the group of K-points of $\overline{G}$ is

$$\overline{G}_K = \{\{\pm\tfrac{1}{\sqrt{b}}B\} : B \in \mathrm{GSO}(f,K) \text{ and } b = \mu(B)\}.$$

Let $C \in \mathrm{GSO}(f,K)$ and $c = \mu(C)$. Then $\frac{1}{\sqrt{c}}C \in \mathrm{SO}(f,\mathbb{R})$. As $(\frac{1}{\sqrt{c}}C)^{-1} = \sqrt{c}\,C^{-1}$, conjugating by $\frac{1}{\sqrt{c}}C$ is the same as conjugating by C, and so by the same argument as in the proof of Lemma 6, we have that $\frac{1}{\sqrt{c}}C$ is in the commensurator $C(\Lambda)$ of Λ in G. Let $C(\overline{\Lambda})$ be the commensurator of $\overline{\Lambda}$ in $\overline{G}$. Then $\overline{G}_K \subseteq C(\overline{\Lambda})$.

The algebraic K-group $\overline{G}$ is K-simple by Lemma 8. The center of $\overline{G}$ is trivial by the proof of Lemma 8, and so $\overline{G}$ is isomorphic to its adjoint group (cf. §3.15 of [7]). The group $\overline{G}_K$ is Zariski-dense in $\overline{G}$ by (3) in §5.4 of [5]. Hence $C(\overline{\Lambda})$ is Zariski-dense in $\overline{G}$, since $\overline{G}_K \subseteq C(\overline{\Lambda})$. Therefore $\overline{\Lambda}$ is Zariski-dense in $\overline{G}$ and $C(\overline{\Lambda}) \subseteq \overline{G}_K$ by the K-version of Lemma 15.11 of [6] (cf. Remarks on p 106 of [6]). As $\overline{\Gamma}_0$ is commensurable to $\overline{\Lambda}$ in $\overline{G}$, we have that

$$\overline{\Gamma}_0 \subseteq C(\overline{\Gamma}_0) = C(\overline{\Lambda}) = \overline{G}_K.$$

There exists $R \in \mathrm{O}(f,K)$ of order 2 with $\det R = -1$ by Theorem 3.20 of [2]. Now R is in the commensurator $\hat{C}(\Lambda)$ of Λ in $\mathrm{O}(f)$ by the argument in the proof of Lemma 6. Let $\overline{R}$ be the image of R in $\mathrm{PO}(f,K)$. Then $\overline{R}$ is in the commensurator $\hat{C}(\overline{\Lambda})$ of $\overline{\Lambda}$ in $\mathrm{PO}(f)$.

Let $\hat{C}(\overline{\Gamma}_0)$ be the commensurator of $\overline{\Gamma}_0$ in $\mathrm{PO}(f)$. Then $\hat{C}(\overline{\Gamma}_0) = \hat{C}(\overline{\Lambda})$, since $\overline{\Gamma}_0$ and $\overline{\Lambda}$ are commensurable. Let $A \in \Gamma'$ with $\det A = -1$, and let $\overline{A} = \psi(A)$. Then $\overline{A} \in \overline{\Gamma}$, and so $\overline{A} \in \hat{C}(\overline{\Gamma}_0)$. Hence $\overline{R}\,\overline{A} \in \hat{C}(\overline{\Gamma}_0)$. As $\det(RA) = 1$, we have that $\overline{R}\,\overline{A} \in C(\overline{\Gamma}_0)$. Hence $\overline{R}\,\overline{A} \in \overline{G}_K$. Therefore $\overline{A} \in \mathrm{PO}(f)_K$ by Lemma 7. Thus $\overline{\Gamma} \subseteq \mathrm{PO}(f)_K$. □

Lemma 10. *Let Γ be an arithmetic group of isometries of H^n of the simplest type defined over K with n odd and $n \geq 3$, and let $\Gamma^{(2)}$ be the subgroup of Γ generated by the squares of elements of Γ. Then $\Gamma^{(2)}$ is a classical arithmetic group of isometries of H^n of the simplest type defined over K.*

Proof. There exists an admissible quadratic form f over K in $n+1$ variables and there exists $M \in \mathrm{GL}(n+1, \mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, and $\Gamma' = M\Gamma M^{-1}$ is commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$ in $\mathrm{O}'(f, \mathbb{R})$. The map $\psi : \mathrm{O}'(f, \mathbb{R}) \to \mathrm{PO}(f, \mathbb{R})$ defined by $\psi(A) = \{\pm A\}$ is an isomorphism. Let $\overline{\Gamma} = \psi(\Gamma')$. We have that $\overline{\Gamma} \subseteq \mathrm{PO}(f)_K$ by Lemma 9, and $\overline{\Gamma}^{(2)} \subseteq \mathrm{PO}(f, K)$ by Lemma 7. Hence $\Gamma'^{(2)} \subseteq \mathrm{O}'(f, K)$, and so $M\Gamma^{(2)}M^{-1} \subseteq \mathrm{O}'(f, K)$. We have that $\Gamma'^{(2)}$ is commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$, since $\Gamma'^{(2)}$ has finite index in Γ'. Thus $\Gamma^{(2)}$ is a classical arithmetic group of isometries of H^n of the simplest type defined over K. □

5. Translation lengths and Salem numbers

There are three types of isometries of hyperbolic n-space H^n, namely elliptic, parabolic, and hyperbolic isometries. An isometry γ of H^n is *elliptic* if γ fixes an actual point of H^n.

An isometry γ of H^n is *parabolic* if γ fixes exactly one ideal point of H^n. There are two types of parabolic isometries of H^n, *parabolic translations* and *loxodromic parabolic* isometries. An isometry γ of H^n is a parabolic translation if in the upper half-space model of hyperbolic n-space, γ is conjugate to a Euclidean translation $\tau(x) = x + a$ with $a \neq 0$.

An isometry γ of H^n is *hyperbolic* if there exists a geodesic in H^n along which γ acts as a translation by a positive distance $\ell(\gamma)$. There are two types of hyperbolic isometries of H^n, *hyperbolic translations* and *loxodromic hyperbolic* isometries. An isometry γ of H^n is a hyperbolic translation if in the upper half-space model of hyperbolic n-space, γ is conjugate to a magnification $\mu(x) = kx$ with $k > 1$.

Let γ be an element of $\mathrm{O}'(n, 1)$. Define the *degree* of γ to be $n+1$. Define the *root of unity degree*, $\deg_1(\gamma)$, of γ to be the number of eigenvalues of γ that are roots of unity. Define the *nonroot of unity degree*, $\deg_\infty(\gamma)$, of γ to be the number of eigenvalues of γ that are not roots of unity. We have that

$$\deg(\gamma) = \deg_1(\gamma) + \deg_\infty(\gamma).$$

Lemma 11. *Let γ be an element of $\mathrm{O}'(n, 1)$. Then $\deg_\infty(\gamma)$ is even, and*

1. *if γ is elliptic, then $\deg_\infty(\gamma) = 0$ if and only if γ has finite order,*
2. *if γ is parabolic, then $\deg_\infty(\gamma) = 0$ if and only if there is a positive integer m such that γ^m is a parabolic translation, and*
3. *if γ is hyperbolic, then $\deg_\infty(\gamma) \geq 2$, and $\deg_\infty(\gamma) = 2$ if and only if there is a positive integer m such that γ^m is a hyperbolic translation.*

Proof. Let $p(x)$ be the characteristic polynomial of γ. Then the eigenvalues of γ are the roots of $p(x)$.

1) First assume that γ is elliptic. Then the roots of $p(x)$ are all complex numbers of absolute value 1 by Proposition 1 of [13]. Hence the roots of $p(x)$ that are not roots of unity are complex and occur in complex conjugate pairs, since $p(x)$ is over $\mathbb{R}$. Therefore $\deg_\infty(\gamma)$ is even. Now γ is diagonalizable over $\mathbb{C}$ by Proposition 1 of [13]. Hence γ has finite order if and only if all the eigenvalues of γ are roots of unity. Therefore $\deg_\infty(\gamma) = 0$ if and only if γ has finite order.

2) Now assume that γ is parabolic. Then the roots of $p(x)$ are all complex numbers of absolute value 1 by Proposition 1 of [13]. Hence the roots of $p(x)$ that are not roots of unity are complex and occur in complex conjugate pairs, since $p(x)$ is over $\mathbb{R}$. Therefore $\deg_\infty(\gamma)$ is even. Now γ is a parabolic translation if and only if all the eigenvalues of γ are 1 by Proposition 1 of [13]. Therefore $\deg_\infty(\gamma) = 0$ if and only if there is a positive integer m such that γ^m is a parabolic translation, since the eigenvalues of γ^m are the mth powers of the eigenvalues of γ.

3) Now assume that γ is hyperbolic. Then the roots of $p(x)$ are $e^{\pm\ell(\gamma)}$, and $(n-1)$ complex numbers of absolute value 1 by Proposition 1 of [13]. Hence the roots of $p(x)$ that are not roots of unity are $e^{\pm\ell(\gamma)}$ and complex roots that occur in complex conjugate pairs, since $p(x)$ is over $\mathbb{R}$. Therefore $\deg_\infty(\gamma)$ is even, and $\deg_\infty(\gamma) \geq 2$. Now γ is diagonalizable over $\mathbb{C}$, and γ is a hyperbolic translation if and only if all the eigenvalues of γ besides $e^{\pm\ell(\gamma)}$ are 1 by Proposition 1 of [13]. Hence $\deg_\infty(\gamma) = 2$ if and only if there is a positive integer m such that γ^m is a hyperbolic translation. □

Lemmas 6 and 10 and the next theorem imply the first half of Theorem 1.

Theorem 4. *Let Γ be a classical arithmetic group of isometries of hyperbolic n-space H^n of the simplest type defined over a totally real number field K. Let γ be a hyperbolic element of Γ, let $\ell(\gamma)$ be the translation length of γ, and let $\lambda = e^{\ell(\gamma)}$. Then*

(1) *λ is a Salem number, and*

$$\deg(\lambda) = \deg_K(\lambda)[K:\mathbb{Q}] \text{ and } \deg_K(\lambda) = \deg_\infty(\gamma) \leq n+1,$$

(2) *K is a subfield of $\mathbb{Q}(\lambda+\lambda^{-1})$, and*

$$[\mathbb{Q}(\lambda+\lambda^{-1}) : K] = \deg_\infty(\gamma)/2 \leq (n+1)/2,$$

(3) *$K = \mathbb{Q}(\lambda+\lambda^{-1})$ if and only if $\deg_\infty(\gamma) = 2$.*

Proof. (1) There exists an admissible quadratic form f over K in $n+1$ variables, and there exists $M \in \mathrm{GL}(n+1,\mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, and $\Gamma' = M\Gamma M^{-1} \subseteq \mathrm{O}'(f,K)$ with Γ' commensurable to $\mathrm{O}'(f,\mathfrak{o}_K)$. Let γ be a hyperbolic element of Γ. Then $\gamma' = M\gamma M^{-1} \in \mathrm{O}'(f,K)$, and there exists a positive integer m such that $(\gamma')^m \in \mathrm{O}'(f,\mathfrak{o}_K)$. Let $p(x)$ be the characteristic polynomial of γ. Then $p(x)$ is the characteristic polynomial of γ'. Hence $p(x)$ is a monic polynomial over $\mathfrak{o}_K$ by Lemma 1. The real roots of $p(x)$ are λ and λ^{-1}, as simple roots, and possibly 1 or -1, as simple or multiple roots, and the complex roots of $p(x)$ occur in complex conjugate pairs of the form $e^{\pm i\theta}$ for some real number θ with $0 < \theta < \pi$ by Proposition 1 of [13].

Let $p(x) = p_1(x)\cdots p_k(x)$ be a factorization of $p(x)$ into a maximum number of monic polynomials over $\mathfrak{o}_K$ of degree at least one. Then $p_j(x)$ is irreducible over $\mathfrak{o}_K$ for each j by Lemma 2. By reindexing if necessary, we may assume that λ^{-1} is a root of $p_1(x)$. Then λ^{-1} is a simple root of $p_1(x)$, and ± 1 is not a root of $p_1(x)$, since otherwise we could factor out $x \pm 1$ from $p_1(x)$ over $\mathfrak{o}_K$.

We claim that $\deg(p_1(x)) > 1$. On the contrary, assume that $p_1(x) = x - \lambda^{-1}$. Then $\lambda^{-1} \in \mathfrak{o}_K$. If $K = \mathbb{Q}$, then $\mathfrak{o}_K = \mathbb{Z}$, and so $\lambda^{-1} \in \mathbb{Z}$, which is a contradiction, since $0 < \lambda^{-1} < 1$. Now assume $K \neq \mathbb{Q}$. Then K has a nonidentity embedding $\sigma : K \to \mathbb{R}$. Let $(\gamma')^\sigma$ be the matrix over $\sigma(K)$ obtained from the matrix γ' over K by applying σ to the entries of γ'. Then $(\gamma')^\sigma \in \mathrm{O}(f^\sigma, \sigma(K))$ and f^σ is positive definite. Hence the roots of the characteristic polynomial $p^\sigma(x)$ of $(\gamma')^\sigma$ are complex numbers of absolute value 1. Therefore the root of $p_1^\sigma(x) = x - \sigma(\lambda^{-1})$ has absolute value 1. Hence $\sigma(\lambda^{-1})$ is a real number of absolute value 1, and so $\sigma(\lambda^{-1}) = \pm 1$, and therefore $\lambda^{-1} = \sigma^{-1}(\pm 1) = \pm 1$, which is a contradiction. Thus $\deg(p_1(x)) > 1$.

We claim that λ is a root of $p_1(x)$. On the contrary, assume that λ is not a root of $p_1(x)$. The complex roots of $p_1(x)$ occur in complex conjugate pairs of the form $e^{\pm i\theta}$ for some real number θ with $0 < \theta < \pi$, since $p_1(x)$ is over $\mathbb{R}$. The constant term of $p_1(x)$ is the product of the negatives of the roots of $p_1(x)$. Hence the constant term of $p_1(x)$ is $-\lambda^{-1}$, which is a contradiction, since $\lambda^{-1} \notin \mathfrak{o}_K$, otherwise we could factor out $x - \lambda^{-1}$ from $p_1(x)$ over $\mathfrak{o}_K$. Therefore λ must also be a root of $p_1(x)$.

Therefore the real roots of $p_1(x)$ are λ and λ^{-1}, and the complex roots of $p_1(x)$ occur in complex conjugate pairs of the form $e^{\pm i\theta}$ with $0 < \theta < \pi$. The polynomial $p_1(x)$ is irreducible over K by Lemma 3, and so $p_1(x)$ is the minimal polynomial of λ over K. Hence $\deg_K(\lambda) = \deg(p_1(x))$.

We claim that no root of $p_1(x)$ is a root of unity. On the contrary, assume that $p_1(x)$ has a root u that is an mth root of unity for some positive integer m. Then $p_1(x)$ is the minimal polynomial of u over K, since $p_1(x)$ is irreducible over K. Now u is a root of $x^m - 1$. Hence $p_1(x)$ divides $x^m - 1$. Therefore all the roots of $p_1(x)$ are roots of unity, which is a contradiction, since λ is not a root of unity. Hence no root of $p_1(x)$ is a root of unity.

There exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ by Theorem 14 on p. 185 of [17]. Let f_α be the minimal polynomial of α over $\mathbb{Q}$, and let $\alpha_1, \ldots, \alpha_d$ be the roots of $f_\alpha(x)$ in $\mathbb{C}$ with $\alpha = \alpha_1$. Then $d = [K : \mathbb{Q}]$. Let $\sigma_1, \ldots, \sigma_d$ be the embeddings of K into $\mathbb{R}$. Then by reindexing, we may assume that $\sigma_j(\alpha) = \alpha_j$ for each j. Then σ_1 is the inclusion $K \subset \mathbb{R}$ and $\sigma_j(K) = \mathbb{Q}(\alpha_j)$ for each j (cf. [17] p 171).

The field $K^* = \mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ is the splitting field of $f_\alpha(x)$. Define the polynomial $p_1^*(x)$ over K^* by the formula

$$p_1^*(x) = p_1^{\sigma_1}(x) \cdots p_1^{\sigma_d}(x).$$

The polynomial $p_1^{\sigma_j}(x)$ is monic for each j, and so $p_1^*(x)$ is monic. The field K^* is a normal extension of $\mathbb{Q}$ by Theorem 4 on p. 175 of [17], and so K^* is a Galois extension of $\mathbb{Q}$.

Let G be the Galois group of K^* over $\mathbb{Q}$, and let $\tau \in G$. Then $(\tau\sigma_1, \ldots, \tau\sigma_d)$ is a permutation of $(\sigma_1, \ldots, \sigma_d)$ (cf. [17] p 182). Hence we have that $(p_1^*)^\tau(x) = p_1^*(x)$ for all $\tau \in G$. Therefore $p_1^*(x)$ is over $\mathbb{Q}$ by Theorem 1 on p. 192 of [17]. Moreover $p_1^*(x)$ is over $\mathbb{A}$, since $p_1(x)$ is over $\mathfrak{o}_K$. Therefore $p_1^*(x)$ is over $\mathbb{Z}$, since $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Assume $j > 1$. The roots of $p_1^{\sigma_j}(x)$ are of the form $e^{i\theta}$ for some real number θ, since $(\gamma')^{\sigma_j} \in \mathrm{O}(f^{\sigma_j}, \sigma_j(K))$ and f^{σ_j} is positive definite. As $p_1^{\sigma_1}(x) = p_1(x)$, we have that λ and λ^{-1} are simple roots of $p_1^*(x)$, and the remaining roots of $p_1^*(x)$ are complex numbers of absolute value 1. Hence $p_1^*(x)$ has all the properties of a Salem polynomial except perhaps irreducibility.

Let $s(x)$ be the minimal polynomial of λ over $\mathbb{Z}$. Then $s(x)$ is irreducible over $\mathbb{Z}$ by Lemma 2. Hence $s(x)$ is irreducible over $\mathbb{Q}$ by Lemma 3. Therefore $s(x)$ is the minimal polynomial of λ over $\mathbb{Q}$. Hence $s(x)$ divides $p_1^*(x)$, and so we can write $p_1^*(x) = s(x)t(x)$ with $t(x)$ a monic polynomial over $\mathbb{Q}$. Let r be a root of $t(x)$. Then r is a root of $p_1^{\sigma_j}(x)$ for some j. Now $p_1^{\sigma_j}(x)$ is irreducible over $\sigma_j(K)$, since $p_1(x)$ is irreducible over K. Hence $p_1^{\sigma_j}(x)$ is the minimal polynomial of r over $\sigma_j(K)$. Therefore $p_1^{\sigma_j}(x)$ divides $t(x)$. Hence $t(x) = p_1^{\sigma_j}(x)h(x)$ with $h(x)$ over

$\sigma_j(K)$. Now we have

$$t(x) = t^{\sigma_j^{-1}}(x) = p_1(x)h^{\sigma_j^{-1}}(x).$$

Hence λ is a root of $t(x)$, which is a contradiction, since λ is a simple root of $p_1^*(x)$. Therefore $t(x) = 1$, and so $s(x) = p_1^*(x)$. Thus $p_1^*(x)$ is irreducible over $\mathbb{Z}$, and so $p_1^*(x)$ is a Salem polynomial with Salem number λ. Moreover, we have that

$$\deg(\lambda) = \deg(p_1^*(x)) = \deg(p_1(x))[K : \mathbb{Q}] = \deg_K(\lambda)[K : \mathbb{Q}].$$

Suppose $j > 1$. We claim that all the roots of $p_j(x)$ are roots of unity. Now all the roots of $p_j(x)$ are of the form $e^{i\theta}$, since the roots of $p_j(x)$ are roots of $p(x)$. Define the polynomial $p_j^*(x)$ over K^* by the formula

$$p_j^*(x) = p_j^{\sigma_1}(x) \cdots p_j^{\sigma_d}(x).$$

The polynomial $p_j^{\sigma_k}(x)$ is monic for each k, and so $p_j^*(x)$ is monic. Each root of $p_j^{\sigma_k}(x)$ is of the form $e^{i\theta}$ for $k > 1$, since $(\gamma')^{\sigma_k} \in \mathrm{O}(f^{\sigma_k}, \sigma_k(K))$ and f^{σ_k} is positive definite. Therefore all the roots of $p_j^*(x)$ are of the form $e^{i\theta}$. By the same argument as with $p_1^*(x)$, we deduce that $p_j^*(x)$ is over $\mathbb{Z}$. Then each root of $p_j^*(x)$ is a root of unity by Kronecker's Theorem [16]. Hence all the roots of $p_j(x)$ are roots of unity. Thus the roots of $p_1(x)$ are precisely the roots of $p(x)$ that are not roots of unity. Therefore

$$\deg_K(\lambda) = \deg(p_1(x)) = \deg_\infty(\gamma) \leq n + 1.$$

(2) The degree of $p_1(x)$ is even, and so there is a positive integer ℓ such that $\deg(p_1(x)) = 2\ell$. By Lemma 4, there exists an irreducible monic polynomial $q(x)$ of degree ℓ over $\mathfrak{o}_K$ such that

$$p_1(x) = x^\ell q(x + x^{-1}).$$

The polynomial $q(x)$ has $\lambda+\lambda^{-1}$ as a root, and $q(x)$ is irreducible over K by Lemma 3. Hence $q(x)$ is the minimal polynomial of $\lambda + \lambda^{-1}$ over K. Therefore

$$[K(\lambda + \lambda^{-1}) : K] = \deg(q(x)) = \deg(p_1(x))/2.$$

Likewise we have

$$\begin{aligned}
[\mathbb{Q}(\lambda + \lambda^{-1}) : \mathbb{Q}] &= \deg(p_1^*(x))/2 \\
&= \deg(p_1(x))[K : \mathbb{Q}]/2 \\
&= [K(\lambda + \lambda^{-1}) : K][K : \mathbb{Q}] \\
&= [K(\lambda + \lambda^{-1}) : \mathbb{Q}].
\end{aligned}$$

As $\mathbb{Q}(\lambda+\lambda^{-1})$ is a subfield of $K(\lambda+\lambda^{-1})$, we deduce that $\mathbb{Q}(\lambda+\lambda^{-1}) = K(\lambda+\lambda^{-1})$. Therefore K is a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$. Moreover, we have that

$$[\mathbb{Q}(\lambda + \lambda^{-1}) : K] = \deg(p_1(x))/2 = \deg_\infty(\gamma)/2 \leq (n + 1)/2.$$

(3) Hence $[\mathbb{Q}(\lambda+\lambda^{-1}) : K] = 1$ if and only if $\deg_\infty(\gamma) = 2$. Thus $K = \mathbb{Q}(\lambda+\lambda^{-1})$ if and only if $\deg_\infty(\gamma) = 2$. □

6. Commensurability classes of Salem numbers

In this section, we prove Theorem 3.

Lemma 12. *If λ is a Salem number of degree d, then*

1. *λ^k is a Salem number of degree d for each positive integer k,*
2. *there exists a unique Salem number λ_1 in $\mathbb{Q}(\lambda)$ such that if μ is a Salem number of degree d in $\mathbb{Q}(\lambda)$, then $\mu = \lambda_1^k$ for some positive integer k, and*
3. *if $\lambda_1 = \mu^k$ for some Salem number μ and positive integer k, then $k = 1$.*

Proof. Assume that $d > 2$. (1) Part (1) is well known. For a proof of (1), see Lemma 2 in [28]. (2) Salem proved Part (2) on p. 167 of [26].

(3) Now $\lambda = \lambda_1^k$ for some positive integer k by (2), and so λ_1 has degree d by (1). Suppose $\lambda_1 = \mu^\ell$ for some Salem number μ and positive integer ℓ. Then μ has degree d by (1). Moreover we have

$$\mathbb{Q}(\mu) = \mathbb{Q}(\mu^\ell) = \mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_1^k) = \mathbb{Q}(\lambda).$$

Hence μ is in $\mathbb{Q}(\lambda)$. Therefore there exists a positive integer m such that $\mu = \lambda_1^m$ by (2). Hence $\lambda_1 = \mu^\ell = \lambda_1^{\ell m}$, and so $\ell = 1$.

Now assume $d = 2$. Let $b = \lambda + \lambda^{-1}$. Then the minimal polynomial of λ over $\mathbb{Z}$ is $x^2 - bx + 1$ with $b > 2$. Hence we have

$$\lambda^{\pm 1} = \big(b \pm \sqrt{b^2 - 4}\big)/2.$$

Write $b^2 - 4 = a^2 D$ with a, D positive integers and D square-free. Then $\mathbb{Q}(\lambda) = \mathbb{Q}(\sqrt{D})$. As $\deg \lambda = 2$, we have that $\lambda \notin \mathbb{Q}$, and so $D > 1$.

Let $K = \mathbb{Q}(\sqrt{D})$. Then every element of $\mathfrak{o}_K$ is of the form $g + h\sqrt{D}$ with $g, h \in \frac{1}{2}\mathbb{Z}$. The *norm* of $g + h\sqrt{D}$ in $\mathfrak{o}_K$ is

$$N(g + h\sqrt{D}) = (g + h\sqrt{D})(g - h\sqrt{D}) = g^2 - h^2 D.$$

The norm is a multiplicative function. Hence if ν is a unit of $\mathfrak{o}_K$, we have that $N(\nu) = \pm 1$.

Let $\nu > 1$ be a unit of $\mathfrak{o}_K$. We claim that ν is a Salem number of degree 2 if and only if $N(\nu) = 1$. First of all $\nu \notin \mathbb{Q}$, since $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. Hence $\deg \nu > 1$, and so $\deg \nu = 2$, since $\mathbb{Q}(\nu) = \mathbb{Q}(\lambda)$. Write $\nu = g + h\sqrt{D}$ with $g, h \in \frac{1}{2}\mathbb{Z}$. Then $h \neq 0$, since $\nu \notin \mathbb{Q}$. Observe that $\nu^{-1} = N(\nu)(g - h\sqrt{D})$ with $N(\nu) = \pm 1$. Suppose that ν is a Salem number of degree 2. Then $\nu + \nu^{-1} \in \mathbb{Z}$, since $x^2 - (\nu + \nu^{-1})x + 1$ is the minimal polynomial of ν over $\mathbb{Z}$. Hence $N(\nu) = 1$, since $2h\sqrt{D} \notin \mathbb{Z}$. Conversely, suppose $N(\nu) = 1$. Then $\nu + \nu^{-1} = 2g \in \mathbb{Z}$, and so $x^2 - (\nu + \nu^{-1})x + 1$ is the minimal polynomial of ν over $\mathbb{Z}$. Therefore ν is a Salem number of degree 2.

(1) Let k be a positive integer. Then λ^k is a unit greater than 1. We have that $N(\lambda^k) = N(\lambda)^k = 1$, and so λ^k is a Salem number of degree 2.

(2) Let $\lambda_0 > 1$ be the fundamental unit of $\mathfrak{o}_K$. Then every unit in $\mathfrak{o}_K$ is of the form $\pm\lambda_0^k$ for some $k \in \mathbb{Z}$. If $N(\lambda_0) = 1$, let $\lambda_1 = \lambda_0$, otherwise let $\lambda_1 = \lambda_0^2$. Then $\lambda_1 > 1$ and $N(\lambda_1) = 1$, and so λ_1 is a Salem number of degree 2.

Let μ be a Salem number of degree 2 in $\mathbb{Q}(\lambda)$. Then μ is a unit greater than 1 such that $N(\mu) = 1$. Hence there exists a positive integer k such that $\mu = \lambda_1^k$.

(3) Part (3) is proved by the same argument as in the case $d > 2$. □

A Salem number λ_1 is said to be *primitive* if whenever $\lambda_1 = \mu^k$ for some Salem number μ and positive integer k, then $k = 1$. If λ is a Salem number, then there exists a unique primitive Salem number λ_1 and a positive integer k such that $\lambda = \lambda_1^k$ by Lemma 12.

We say that Salem numbers λ and μ are *commensurable* if there exists positive integers k and ℓ such that $\lambda^k = \mu^\ell$. Commensurability is an equivalence relation on the set of all Salem numbers, since if λ, μ, ν are Salem numbers and k, ℓ, m, n are positive integers such that $\lambda^k = \mu^\ell$ and $\mu^m = \nu^n$, then $\lambda^{km} = \mu^{\ell m} = \nu^{\ell n}$.

Lemma 13. *Let λ be a Salem number, let $\langle\lambda\rangle$ be the commensurability class of λ, and let λ_1 be the unique primitive Salem number such that $\lambda = \lambda_1^k$ for some integer k. Then $\langle\lambda\rangle = \{\lambda_1^n : n$ is a positive integer$\}$.*

Proof. If n is a positive integer, then $(\lambda_1^n)^k = \lambda^n$, and so $\lambda_1^n \in \langle\lambda\rangle$. Let $\mu \in \langle\lambda\rangle$. Then there exists positive integers ℓ and m such that $\lambda^\ell = \mu^m$. Let μ_1 be the unique primitive Salem number such that $\mu = \mu_1^n$ for some positive integer n. Then we have that $\lambda_1^{k\ell} = \mu_1^{mn}$. By Lemma 12(1), we have that

$$\mathbb{Q}(\lambda_1) = \mathbb{Q}(\lambda_1^{k\ell}) = \mathbb{Q}(\mu_1^{mn}) = \mathbb{Q}(\mu_1).$$

Hence $\lambda_1 = \mu_1$ by Lemma 12. Therefore $\mu \in \{\lambda_1^n : n \text{ is a positive integer}\}$. □

It follows from Lemma 13, that $\langle\lambda\rangle \mapsto \lambda_1$ is a bijection from the set of commensurability classes of Salem numbers to the the set of primitive Salem numbers. The next theorem is an enhanced version of Theorem 3.

Theorem 5. *Let Γ be an arithmetic group of isometries of H^n, with $n > 1$, of the simplest type defined over a totally real number field K. Then there exists infinitely many commensurability classes of Salem numbers of the form $e^{\ell(\gamma)}$ for some hyperbolic translation γ in Γ.*

Proof. Assume first that $n = 2$. On the contrary, assume that there are only finitely many commensurability classes of Salem numbers of the form $e^{\ell(\gamma)}$ for some hyperbolic translation γ in Γ. Let Λ_1 be the finite set of corresponding primitive Salem numbers. Let γ be a hyperbolic element of Γ. Then γ is either a hyperbolic translation or a glide reflection. In the latter case γ^2 is a hyperbolic translation. Now γ is an element of the matrix group $\mathrm{O}'(2,1)$. The eigenvalues of γ are of the form ± 1 and $\lambda^{\pm 1}$ for a Salem number $\lambda = e^{\ell(\gamma)}$ by Lemma 6 and Theorem 4. We have that $\lambda^2 = e^{2\ell(\gamma)} = e^{\ell(\gamma^2)}$ with γ^2 a hyperbolic translation. Hence there exists $\lambda_1 \in \Lambda_1$ and a positive integer k such that $\lambda = \lambda_1^k$ by Lemma 13.

All parabolic elements of Γ are parabolic translations, and so have all eigenvalues equal to 1. All elliptic elements of Γ have finite order, since Γ is discrete. Now H^2/Γ has finite area, and so Γ is finitely generated by Theorem 10.1.2 of [3]. Hence there are only finitely many conjugacy classes of elements of Γ of finite order by Corollary 10.3.3 of [3]. Let Θ be the set of all the eigenvalues of all the elliptic elements of Γ. Then Θ is a finite set of roots of unity by Lemma 11(1). Therefore $[\mathbb{Q}(\Lambda_1 \cup \Theta) : \mathbb{Q}]$ is finite by Proposition 5 on p. 165 of [17], since $\Lambda_1 \cup \Theta$ is a finite subset of $\mathbb{A}$.

Let evΓ be the set of all the eigenvalues of elements of Γ. Then we have

$$\mathbb{Q}(\mathrm{ev}\Gamma) \subseteq \mathbb{Q}(\Lambda_1 \cup \Theta).$$

Hence $[\mathbb{Q}(\mathrm{ev}\Gamma) : \mathbb{Q}]$ is finite. However $[\mathbb{Q}(\mathrm{ev}\Gamma) : \mathbb{Q}]$ is infinite by Theorem 3.1 of [14]. Therefore there must be infinitely many commensurability classes of Salem numbers λ of the form $e^{\ell(\gamma)}$ for some hyperbolic translation γ in Γ.

Assume now that $n > 2$. Then there exists an admissible quadratic form f over K in $n + 1$ variables, and there exists $M \in \mathrm{GL}(n + 1, \mathbb{R})$ such that $f(Mx) = f_n(x)$

for all $x \in \mathbb{R}^{n+1}$, and $M\Gamma M^{-1}$ is commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$ in $\mathrm{O}'(f, \mathbb{R})$. We have that $M^{-1}\mathrm{O}'(f,\mathbb{R})M = \mathrm{O}'(n,1)$, and Γ is commensurable to $M^{-1}\mathrm{O}'(f,\mathfrak{o}_K)M$ in $\mathrm{O}'(n,1)$.

The form f can be diagonalized over K. Let A be the $(n+1)\times(n+1)$ coefficient matrix of f. Then there is a matrix $C \in \mathrm{GL}(n+1, K)$ and a diagonal matrix D such that $C^tAC = D$ by Corollary on p. 107 of [24]. Moreover D is the coefficient matrix of a diagonal quadratic form f' equivalent to f over K with $f(Cx) = f'(x)$ for all $x \in \mathbb{R}^{n+1}$. The quadratic form f' is also admissible, since for each nonidentity embedding $\sigma : K \to \mathbb{R}$, we have that $(C^\sigma)^t A^\sigma C^\sigma = D^\sigma$, and D^σ is the matrix of $(f')^\sigma$.

We have that $C^{-1}\mathrm{O}'(f,K)C = \mathrm{O}'(f',K)$. The group $C^{-1}\mathrm{O}'(f,\mathfrak{o}_K)C$ is commensurable to $\mathrm{O}'(f',\mathfrak{o}_K)$ by Lemma 2.2 of [1]. Hence $M^{-1}\mathrm{O}'(f,\mathfrak{o}_K)M$ is commensurable to $M^{-1}C\mathrm{O}'(f',\mathfrak{o}_K)C^{-1}M$ in $\mathrm{O}'(n,1)$.

Suppose

$$f'(x) = a_1x_1^2 + \cdots + a_{n+1}x_{n+1}^2.$$

As the signature of f' is $(n,1)$, exactly one coefficient a_i is negative and the rest are positive. By permuting coordinates, we may assume that a_{n+1} is negative.

Let B be the $(n+1)\times(n+1)$ diagonal matrix defined by

$$B = \mathrm{diag}\big(a_1^{-1/2}, \dots, a_n^{-1/2}, (-a_{n+1})^{-1/2}\big).$$

Then $f'(Bx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$. Let $\Gamma' = B^{-1}\mathrm{O}'(f',\mathfrak{o}_K)B$. Then Γ' is an arithmetic group of isometries of H^n of the simplest type over K. We have that

$$M^{-1}C\mathrm{O}'(f',\mathfrak{o}_K)C^{-1}M = M^{-1}CB\Gamma'B^{-1}C^{-1}M,$$

and Γ is commensurable to $M^{-1}CB\Gamma'B^{-1}C^{-1}M$ in $\mathrm{O}'(n,1)$. As $f(Mx) = f_n(x) = f'(Bx)$ and $f(Cx) = f'(x)$, we have that $f_n(B^{-1}C^{-1}Mx) = f_n(x)$. Hence we have that $\pm B^{-1}C^{-1}M \in \mathrm{O}'(n,1)$. In other words, Γ is commensurable to Γ' in $\mathrm{O}'(n,1)$ in the wide sense.

The binary quadratic form

$$f_2'(x) = a_{n-1}x_{n-1}^2 + a_nx_n^2 + a_{n+1}x_{n+1}^2$$

over K is admissible. Let B_2 be the 3×3 diagonal matrix defined by

$$B_2 = \mathrm{diag}\big(a_{n-1}^{-1/2}, a_n^{-1/2}, (-a_{n+1})^{-1/2}\big).$$

Then $f_2'(B_2x) = f_2(x)$ for all $x \in \mathbb{R}^3$. Let $\Gamma_2' = B_2^{-1}\mathrm{O}'(f_2',\mathfrak{o}_K)B_2$. Then Γ_2' is an arithmetic group of isometries of H^2 of the simplest type over K. Hence there are infinitely many commensurability classes of Salem numbers of the form $e^{\ell(\gamma')}$ for some hyperbolic translation γ' in Γ_2' by the case $n = 2$.

Let $\hat{\mathrm{O}}'(f_2',\mathfrak{o}_K)$ be the group of $(n+1)\times(n+1)$ block diagonal matrices with blocks the $(n+1-3)\times(n+1-3)$ identity matrix and a matrix in $\mathrm{O}'(f_2', \mathrm{o}_K)$. Then $\hat{\mathrm{O}}'(f_2',\mathfrak{o}_K)$ is a subgroup of $\mathrm{O}'(f',\mathfrak{o}_K)$. Let $\hat{\Gamma}_2' = B^{-1}\hat{\mathrm{O}}'(f_2',\mathfrak{o}_K)B$. If γ' is a hyperbolic translation in Γ_2' and $\hat{\gamma}'$ is the corresponding element of $\hat{\Gamma}_2'$, then $\hat{\gamma}'$ is a hyperbolic translation in $\hat{\Gamma}_2'$ by Proposition 1 of [13]. Hence $\hat{\Gamma}_2'$ is a subgroup of Γ' with infinitely many commensurability classes of Salem numbers of the form $e^{\ell(\hat{\gamma}')}$ for some hyperbolic translation $\hat{\gamma}'$ in $\hat{\Gamma}_2'$. Therefore there are infinitely many commensurability classes of Salem numbers of the form $e^{\ell(\gamma)}$ for some hyperbolic translation γ in Γ. □

7. Salem numbers and translation lengths

In this section, we prove the second half of Theorem 1 and provide a sharp example for Corollary 2 in dimension 2.

Lemma 14. *If λ is a Salem number and K is a subfield of $\mathbb{Q}(\lambda+\lambda^{-1})$, then*

$$\deg(\lambda) = \deg_K(\lambda)[K:\mathbb{Q}].$$

Proof. As $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\lambda+\lambda^{-1})$, we have that

$$\mathbb{Q}(\lambda) \subseteq K(\lambda) \subseteq \mathbb{Q}(\lambda+\lambda^{-1})(\lambda) = \mathbb{Q}(\lambda),$$

and so $\mathbb{Q}(\lambda) = K(\lambda)$. Therefore we have that

$$\begin{aligned} \deg(\lambda) &= [\mathbb{Q}(\lambda):\mathbb{Q}] \\ &= [\mathbb{Q}(\lambda):K][K:\mathbb{Q}] \\ &= [K(\lambda):K][K:\mathbb{Q}] \quad = \quad \deg_K(\lambda)[K:\mathbb{Q}]. \end{aligned}$$ □

Theorem 6. *Let λ be a Salem number, let K be a subfield of $\mathbb{Q}(\lambda+\lambda^{-1})$, and let n be a positive integer such that $\deg_K(\lambda) \leq n+1$. Then there exists a classical arithmetic group Γ of isometries of H^n of the simplest type over K and an orientation preserving hyperbolic element γ of Γ such that $\lambda = e^{\ell(\gamma)}$.*

Proof. Let $p(x)$ be the minimal polynomial of λ over K, and let $s(x)$ be the Salem polynomial of λ. Then $p(x)$ divides $s(x)$, and so the roots of $p(x)$ are roots of $s(x)$. Hence the roots of $p(x)$ are in $\mathbb{A}$. Therefore $p(x)$ is over $\mathfrak{o}_K$.

The complex roots of $p(x)$ occur in complex conjugate pairs of the form $e^{\pm i\theta}$ for some real number θ with $0 < \theta < \pi$, since $p(x)$ is over $\mathbb{R}$. Now $\lambda \notin K$, since $[\mathbb{Q}(\lambda):\mathbb{Q}(\lambda+\lambda^{-1})] = 2$ by Lemma 4. Hence λ^{-1} is a root of $p(x)$, since otherwise the constant term of $p(x)$ would be $-\lambda$, which is not the case, since $\lambda \notin K$.

Therefore the real roots of $p(x)$ are $\lambda^{\pm 1}$, and the complex roots occur in complex conjugate pairs of the form $e^{\pm i\theta}$ with $0 < \theta < \pi$. The roots of $p(x)$ are simple, since $p(x)$ is irreducible over K. Let $m = \deg(p(x))$. Then m is even, say $m = 2\ell$. Let $r_1, \ldots, r_m$ be the roots of $p(x)$ with $r_{2j-1} = e^{-i\theta_j}$ and $r_{2j} = e^{i\theta_j}$, with $0 < \theta_j < \pi$, for $j = 1, \ldots, \ell-1$, and $r_{m-1} = \lambda^{-1}$ and $r_m = \lambda$.

Let $\eta = \log\lambda$. Then $\lambda = e^\eta$. Let M be the block diagonal $m \times m$ matrix with blocks

$$\begin{pmatrix} \cos\theta_j & -\sin\theta_j \\ \sin\theta_j & \cos\theta_j \end{pmatrix} \quad \text{for} \quad 1 \leq j < \ell, \quad \text{and} \quad \begin{pmatrix} \cosh\eta & \sinh\eta \\ \sinh\eta & \cosh\eta \end{pmatrix}.$$

Then M is a hyperbolic element of $\mathrm{O}'(m-1,1)$ with characteristic polynomial $p(x)$, since the eigenvalues of M are $e^{\pm i\theta_1}, \ldots, e^{\pm i\theta_{\ell-1}}$, and $e^{\pm\eta}$. Moreover $\det M = 1$, and so M is an orientation preserving isometry of H^n.

Define a vector v in $\mathbb{R}^m$ by

$$v = (1,0,1,0,\ldots,1,0).$$

Let $w_j = M^{j-1}v$ for $j = 1, \ldots, m$. Then w_j is the vector

$$\big(\cos(j-1)\theta_1, \sin(j-1)\theta_1, \ldots, \cos(j-1)\theta_{\ell-1}, \sin(j-1)\theta_{\ell-1}, \cosh(j-1)\eta, \sinh(j-1)\eta\big).$$

Let W be the $m \times m$ matrix whose jth column vector is w_j. We claim that W is invertible.

Let B be the block diagonal $m \times m$ matrix with the first $m-1$ blocks

$$\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} \quad \text{and last block} \quad \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

We have that $\det(B) = i^{\ell-1}2^{\ell}$. Observe that

$$\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}\begin{pmatrix} \cos(2k-1)\theta_j & \cos 2k\theta_j \\ \sin(2k-1)\theta_j & \sin 2k\theta_j \end{pmatrix} = \begin{pmatrix} e^{-(2k-1)i\theta_j} & e^{-2ki\theta_j} \\ e^{(2k-1)i\theta_j} & e^{2ki\theta_j} \end{pmatrix},$$

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \cosh(2k-1)\eta & \cosh 2k\eta \\ \sinh(2k-1)\eta & \sinh 2k\eta \end{pmatrix} = \begin{pmatrix} e^{-(2k-1)\eta} & e^{-2k\eta} \\ e^{(2k-1)\eta} & e^{2k\eta} \end{pmatrix}.$$

Therefore we have that

$$BW = \begin{pmatrix} 1 & r_1 & r_1^2 & \cdots & r_1^{m-1} \\ 1 & r_2 & r_2^2 & \cdots & r_2^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & r_m & r_m^2 & \cdots & r_m^{m-1} \end{pmatrix}.$$

Hence BW is a Vandermonde $m \times m$ matrix. Therefore we have

$$\det(BW) = \prod_{1 \leq j < k \leq m} (r_k - r_j),$$

and so W is invertible, since the roots $r_1, \ldots, r_m$ of $p(x)$ are distinct.

Define an $m \times m$ matrix C by the formula $C = W^{-1}MW$. Let $e_1, \ldots, e_m$ be the standard basis vectors of $\mathbb{R}^m$. Then for $j < m$, we have that

$$Ce_j = W^{-1}MWe_j = W^{-1}Mw_j = W^{-1}w_{j+1} = e_{j+1}.$$

Therefore C is of the form

$$C = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_1 \\ 1 & 0 & \cdots & 0 & c_2 \\ 0 & 1 & \cdots & 0 & c_3 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_m \end{pmatrix}.$$

The matrix C has the same characteristic polynomial as M. Hence C must be the companion matrix of $p(x)$, and so if

$$p(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m,$$

then $c_j = -a_{j-1}$ for $j = 1, \ldots, m$. Therefore C is over $\mathfrak{o}_K$.

Define an $m \times m$ diagonal matrix J by

$$J = \mathrm{diag}(1, \ldots, 1, -1).$$

Then J is the coefficient matrix of the Lorentzian quadratic form $f_{m-1}(x)$. Define a symmetric $m \times m$ matrix A by the formula $A = W^tJW$. Then A is the coefficient matrix of a quadratic form f over $\mathbb{R}$ in m variables. If $x \in \mathbb{R}^m$, then

$$f(x) = x^tAx = x^tW^tJWx = (Wx)^tJWx = f_{m-1}(Wx),$$

and so f has signature $(m-1, 1)$ and

$$\mathrm{O}'(f, \mathbb{R}) = W^{-1}\mathrm{O}'(m-1,1)W.$$

Now $M \in \mathrm{O}'(m-1,1)$ and $C = W^{-1}MW$. Hence $C \in \mathrm{O}'(f, \mathfrak{o}_K)$.

We claim that f is over K. If $x, y \in \mathbb{R}^m$, define the *Lorentzian inner product* of x and y to be $x \circ y = x^t Jy$. Let $A = (a_{jk})$. Then we have that $a_{jk} = w_j \circ w_k$. The matrix M preserves the Lorentzian inner product. Hence if $j, k < m$, we have that

$$a_{j+1,k+1} = w_{j+1} \circ w_{k+1} = Mw_j \circ Mw_k = w_j \circ w_k = a_{jk}.$$

Therefore the entries of A are all the same on the main diagonal and on all offset diagonals. As A is symmetric, to determine A it suffices to determine the first column of A, that is, to determine a_{j1} for $j = 1, \ldots, m$. We have that

$$a_{j1} = w_j \circ v = \cos(j-1)\theta_1 + \cdots + \cos(j-1)\theta_{\ell-1} + \cosh(j-1)\eta.$$

For $j = 1$, we see that all the elements on the main diagonal of A are equal to ℓ. Now we have

$$\begin{aligned} r_{2k-1}^{j-1} &= \cos(j-1)\theta_k - i\sin(j-1)\theta_k \\ r_{2k}^{j-1} &= \cos(j-1)\theta_k + i\sin(j-1)\theta_k, \end{aligned}$$

and so

$$\cos(j-1)\theta_k = (r_{2k-1}^{j-1} + r_{2k}^{j-1})/2.$$

Likewise we have

$$\begin{aligned} r_{m-1}^{j-1} &= \cosh(j-1)\eta - \sinh(j-1)\eta \\ r_{m}^{j-1} &= \cosh(j-1)\eta + \sinh(j-1)\eta, \end{aligned}$$

and so

$$\cosh(j-1)\eta = (r_{m-1}^{j-1} + r_m^{j-1})/2.$$

Therefore we have that

$$a_{j1} = (r_1^{j-1} + \cdots + r_m^{j-1})/2.$$

Now $r_1^{j-1} + \cdots + r_m^{j-1}$ is equal to the symmetric polynomial $x_1^{j-1} + \cdots + x_m^{j-1}$ evaluated at the roots $r_1, \ldots, r_m$ of $p(x)$. Let $s_k(x_1, \ldots, x_m)$ be the kth elementary symmetric polynomial in m variables, and let

$$t_k = s_k(r_1, \ldots, r_m).$$

Then we have that

$$p(x) = x^m - t_1x^{m-1} + \cdots + (-1)^m t_m,$$

and so $t_k \in \mathfrak{o}_K$ for each $k = 1, \ldots, m$. By Newton's identities there is a polynomial $g_j(x_1, \ldots, x_m)$ over $\mathbb{Z}$ such that

$$x_1^j + \cdots + x_m^j = g_j(s_1(x_1, \ldots, x_m), \ldots, s_m(x_1, \ldots, x_m)).$$

Hence we have

$$r_1^{j-1} + \cdots + r_m^{j-1} = g_{j-1}(t_1, \ldots, t_m).$$

Therefore $r_1^{j-1} + \cdots + r_m^{j-1} \in \mathfrak{o}_K$. Hence $2A$ is over $\mathfrak{o}_K$, and so A is over K. Therefore the quadratic form f is over K. In fact f has collected coefficients in $\mathfrak{o}_K$, since $a_{jj} = \ell$ and if $j \neq k$, then $a_{jk} + a_{kj} \in \mathfrak{o}_K$.

We next show that f is admissible. This is clear if $K = \mathbb{Q}$, and so assume $K \neq \mathbb{Q}$. Every embedding of K into $\mathbb{C}$ extends to an embedding of $\mathbb{Q}(\lambda + \lambda^{-1})$ into $\mathbb{C}$ by Proposition 8 on p. 171 of [17]. As $\mathbb{Q}(\lambda + \lambda^{-1})$ is totally real, K is also totally real.

Let $d = [K : \mathbb{Q}]$, and let $\sigma_1, \ldots, \sigma_d$ be the embeddings of K into $\mathbb{R}$ with σ_1 the inclusion of K into $\mathbb{R}$. Define the monic polynomial $p^*(x)$ by the formula

$$p^*(x) = p^{\sigma_1}(x) \cdots p^{\sigma_d}(x).$$

By Lemma 14, we have

$$\deg(p^*(x)) = \deg(p(x))d = \deg_K(\lambda)[K : \mathbb{Q}] = \deg(\lambda) = \deg(s(x)).$$

By the Galois group argument in the proof of Theorem 4, we deduce that $p^*(x)$ is over $\mathbb{Q}$. Now $s(x)$ divides $p^*(x)$, since $s(x)$ is the minimal polynomial of λ over $\mathbb{Q}$. Therefore $s(x) = p^*(x)$, since $\deg(s(x)) = \deg(p^*(x))$.

Assume that $j > 1$. Then the roots of $p^{\sigma_j}(x)$ are simple complex roots that occur in complex conjugate pairs of the form $e^{\pm i\theta}$ for some real number θ. Define an $m \times m$ block diagonal matrix M_j in terms of the roots of $p^{\sigma_j}(x)$ in the same way that we defined M . Then M_j is a rotation matrix. Define an $m \times m$ matrix W_j in terms of M_j and v in the same way that we defined W. Then W_j is invertible by the same Vandermonde determinant argument. Define an $m \times m$ symmetric matrix A_j by the formula $A_j = W_j^t W_j$. Then the quadratic form f_j, whose coefficient matrix is A_j, is positive definite. The entries of A_j are expressed in terms of the coefficients of $p^{\sigma_j}(x)$ in the same way that the entries of A are expressed in terms of the coefficients of $p(x)$. Hence $A_j = A^{\sigma_j}$ and so $f_j = f^{\sigma_j}$. Therefore f^{σ_j} is positive definite. Thus f is admissible.

Let $\Gamma = W\mathrm{O}'(f, \mathfrak{o}_K)W^{-1}$. Then Γ is a classical arithmetic group of isometries of H^{m-1} of the simplest type over K. We have that $\gamma = M = WCW^{-1}$ is an orientation preserving hyperbolic element of Γ such that $\lambda = e^{\ell(\gamma)}$. If $n = m - 1$, we are done, so assume that $n > m - 1$.

If X is an $m \times m$ matrix, let $\hat{X}$ be the block diagonal $(n + 1) \times (n + 1)$ matrix with blocks the $(n + 1 - m) \times (n + 1 - m)$ identity matrix and X. Then $\hat{J}$ is the coefficient matrix of the Lorentzian quadratic form $f_n(x)$. We have that $\hat{M}^t\hat{J}\hat{M} = \hat{J}$ and $\hat{M} \in \mathrm{O}'(n, 1)$. The matrix $\hat{W}$ is invertible and $\hat{C} = \hat{W}^{-1}\hat{M}\hat{W}$ and $\hat{A} = \hat{W}^t\hat{J}\hat{W}$ and $\hat{C}^t\hat{A}\hat{C} = \hat{A}$, with $\hat{C}$ over $\mathfrak{o}_K$ and $\hat{A}$ over K. Let $\hat{f}$ be the quadratic form whose coefficient matrix is $\hat{A}$. Then $\hat{f}$ is over K.

The quadratic form $\hat{f}$ has signature $(n, 1)$, since $f(x) = f_n(\hat{W}x)$ for all $x \in \mathbb{R}^{n+1}$. Moreover $\hat{C} \in \mathrm{O}'(\hat{f}, \mathfrak{o}_K)$. Assume $j > 1$. Let $\hat{f}_j$ be the quadratic form whose coefficient matrix is $\hat{A}_j$. Then $\hat{f}_j$ is positive definite and $\hat{f}_j = (\hat{f})^{\sigma_j}$. Therefore $\hat{f}$ is admissible. Let $\hat{\Gamma} = \hat{W}\mathrm{O}'(\hat{f}, \mathfrak{o}_K)\hat{W}^{-1}$. Then $\hat{\Gamma}$ is a classical arithmetic group of isometries of H^n of the simplest type over K with an orientation preserving hyperbolic element $\hat{\gamma} = \hat{M} = \hat{W}\hat{C}\hat{W}^{-1}$ such that $\lambda = e^{\ell(\hat{\gamma})}$. □

The next corollary is a enhanced version of Corollary 1.

Corollary 5. *Let λ be a Salem number. Then for each integer $n > 0$, there exists a classical arithmetic group Γ of isometries of H^n of simplest type defined over $\mathbb{Q}(\lambda + \lambda^{-1})$ and a hyperbolic translation γ in Γ such that $\lambda = e^{\ell(\gamma)}$.*

Proof. Let $K = \mathbb{Q}(\lambda + \lambda^{-1})$. Then the minimal polynomial of λ over K is

$$p(x) = (x - \lambda)(x - \lambda^{-1}) = x^2 - (\lambda + \lambda^{-1})x + 1.$$

Hence $\deg_K(\lambda) = 2$, and so $\deg_K(\lambda) \leq n + 1$ for each positive integer n. Therefore there exists a classical arithmetic group Γ of isometries of H^n of the simplest type over K and a hyperbolic element γ of Γ such that $\lambda = e^{\ell(\gamma)}$ by Theorem 6. Moreover γ is a hyperbolic translation by the proof of Theorem 6, since $\deg(p(x)) = 2$. □

The next corollary follows from Lemma 6 and Theorems 4 and 6.

Corollary 6. *Let Γ be an arithmetic group of isometries of H^n of the simplest type defined over $\mathbb{Q}$, with n even, and let C be a closed geodesic in H^n/Γ. Then* $\mathrm{length}(C) \geq b_n$*, and this lower bound is sharp for each even positive integer n.*

Corollary 2 follows from Corollary 6 once we have a sharp non-cocompact example for $n = 2$, since all arithmetic groups of isometries of H^n of the simplest type over $\mathbb{Q}$ are not cocompact when $n > 3$. Now $\lambda + \lambda^{-1}$ is an increasing function of λ for $\lambda > 1$, and so λ is an increasing function of $\lambda + \lambda^{-1}$ for $\lambda + \lambda^{-1} > 2$. Therefore the smallest Salem number λ_1 of degree 2 occurs when $\lambda_1 + \lambda_1^{-1} = 3$, and so

$$\lambda_1 = \big(3 + \sqrt{5}\big)/2 = 2.618033988\ldots\ ,$$

and we have that

$$b_1 = b_2 = \log(\lambda_1) = .9624236501\ldots\ .$$

When $n = 2$ and $\lambda = \lambda_1$, the proof of Theorem 6 yields the quadratic form

$$f(x) = x_1^2 + x_2^2 + 3x_2x_3 + x_3^2.$$

Now $f(1, -1, 2) = 0$, and so a corresponding arithmetic group Γ of isometries of H^2 is not cocompact. Thus we have a sharp example for Corollary 2 when $n = 2$.

8. Square-rootable Salem numbers

In this section, we prove Theorem 2. The first half of Theorem 2 is Theorem 7 and the second half of Theorem 2 is Theorem 8 below.

Lemma 15. *Let λ be a Salem number. Then* $\deg \lambda^{\frac{1}{2}} = \deg \lambda$ *or* $2 \deg \lambda$*. Moreover* $\deg \lambda^{\frac{1}{2}} = \deg \lambda$ *if and only if either $\lambda^{\frac{1}{2}}$ is a Salem number or* $\deg \lambda^{\frac{1}{2}} = 2$ *and the norm of $\lambda^{\frac{1}{2}}$ is -1.*

Proof. We have that $\mathbb{Q}(\lambda^{\frac{1}{2}}) = \mathbb{Q}(\lambda)(\lambda^{\frac{1}{2}})$. Hence $\mathbb{Q}(\lambda^{\frac{1}{2}}) = \mathbb{Q}(\lambda)$ if $\lambda^{\frac{1}{2}} \in \mathbb{Q}(\lambda)$ or else $\mathbb{Q}(\lambda^{\frac{1}{2}})$ is a quadratic extension of $\mathbb{Q}(\lambda)$ if $\lambda^{\frac{1}{2}} \notin \mathbb{Q}(\lambda)$. Therefore we have that

$$\deg \lambda^{\frac{1}{2}} = [\mathbb{Q}(\lambda^{\frac{1}{2}}) : \mathbb{Q}] = [\mathbb{Q}(\lambda^{\frac{1}{2}}) : \mathbb{Q}(\lambda)][\mathbb{Q}(\lambda) : \mathbb{Q}] = \epsilon \deg \lambda$$

with $\epsilon = 1$ or 2 depending on whether or not $\lambda^{\frac{1}{2}} \in \mathbb{Q}(\lambda)$.

Suppose $\deg \lambda^{\frac{1}{2}} = \deg \lambda$. Let $s(x)$ be the Salem polynomial of λ and let $p(x)$ be the minimal polynomial of $\lambda^{\frac{1}{2}}$ over $\mathbb{Z}$. Then $p(x)$ is the minimal polynomial of $\lambda^{\frac{1}{2}}$ over $\mathbb{Q}$ by Lemma 3. Hence $\deg p(x) = \deg s(x)$.

As $\lambda^{\frac{1}{2}}$ is a root of $s(x^2)$, we have that $s(x^2) = p(x)q(x)$ for some $q(x)$ over $\mathbb{Z}$. The roots of $s(x^2)$ are of the form $\pm r^{\frac{1}{2}}$ where r is a root of $s(x)$. None of the roots of $s(x)$ are roots of unity. Hence $q(x)$ must have a real root by Kronecker's theorem [16]. As $\deg q(x) = \deg p(x) = \deg s(x)$, we have that $\deg q(x)$ is even. Therefore $q(x)$ has two real roots and $p(x)$ has two real roots, since $s(x^2)$ has four real roots.

Suppose $\deg s(x) \geq 4$. Then $p(x)$ has a pair of reciprocal complex roots, and so $p(x) = x^m p(x^{-1})$ with $m = \deg p(x)$, whence all the roots of $p(x)$ occur in reciprocal pairs. Therefore $p(x)$ is a Salem polynomial, and so $\lambda^{\frac{1}{2}}$ is a Salem number.

Now suppose $\deg s(x) = 2$. If the other root of $p(x)$ is $\lambda^{-\frac{1}{2}}$, then $\lambda^{\frac{1}{2}}$ is a Salem number. The other root of $p(x)$ cannot be $-\lambda^{\frac{1}{2}}$ otherwise the constant term of $p(x)$ would be $-\lambda$ which is not an integer. Hence if $\lambda^{\frac{1}{2}}$ is not a Salem number, then the other root of $p(x)$ must be $-\lambda^{-\frac{1}{2}}$, and therefore the norm of $\lambda^{\frac{1}{2}}$ is -1.

Conversely, if $\lambda^{\frac{1}{2}}$ is a Salem number, then $\deg \lambda = \deg \lambda^{\frac{1}{2}}$ by Lemma 12(1). If $\deg \lambda^{\frac{1}{2}} = 2$ and the norm of $\lambda^{\frac{1}{2}}$ is -1, then $\deg \lambda = 2 = \deg \lambda^{\frac{1}{2}}$. □

Lemma 16. *If λ be a Salem number and K is a subfield of $\mathbb{Q}(\lambda+\lambda^{-1})$, then*

$$\deg(\lambda^{\frac{1}{2}}) = \deg_K(\lambda^{\frac{1}{2}})[K:\mathbb{Q}].$$

Proof. As $(\lambda^{\frac{1}{2}}+\lambda^{-\frac{1}{2}})^2 = \lambda+2+\lambda^{-1}$, we have that

$$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\lambda+\lambda^{-1}) \subseteq \mathbb{Q}(\lambda^{\frac{1}{2}}+\lambda^{-\frac{1}{2}}).$$

Hence we have that

$$\mathbb{Q}(\lambda^{\frac{1}{2}}) \subseteq K(\lambda^{\frac{1}{2}}) \subseteq \mathbb{Q}(\lambda^{\frac{1}{2}}+\lambda^{-\frac{1}{2}})(\lambda^{\frac{1}{2}}) = \mathbb{Q}(\lambda^{\frac{1}{2}}),$$

and so $\mathbb{Q}(\lambda^{\frac{1}{2}}) = K(\lambda^{\frac{1}{2}})$.

Therefore we have that

$$\begin{aligned}\deg(\lambda^{\frac{1}{2}}) &= [\mathbb{Q}(\lambda^{\frac{1}{2}}):\mathbb{Q}]\\ &= [\mathbb{Q}(\lambda^{\frac{1}{2}}):K][K:\mathbb{Q}]\\ &= [K(\lambda^{\frac{1}{2}}):K][K:\mathbb{Q}] \quad = \quad \deg_K(\lambda^{\frac{1}{2}})[K:\mathbb{Q}]. \qquad \square\end{aligned}$$

Let λ be a Salem number, let K be a subfield of $\mathbb{Q}(\lambda+\lambda^{-1})$, and let $p(x)$ be the minimal polynomial of λ over K. We say that λ is *square-rootable over K* if there exists a totally positive element α of K and a monic palindromic polynomial $q(x)$, whose even degree coefficients are in K and whose odd degree coefficients are in $\sqrt{\alpha}K$, such that $q(x)q(-x) = p(x^2)$. We also say that λ is *square-rootable over K* via α.

Lemma 17. *Let λ be a Salem number and let K be a subfield of $\mathbb{Q}(\lambda+\lambda^{-1})$. Then λ is square-rootable over K via a square in K if and only if $\lambda^{\frac{1}{2}}$ is a Salem number.*

Proof. Let $p(x)$ be the minimal polynomial of λ over K. First assume that $\lambda^{\frac{1}{2}}$ is a Salem number. Let $q(x)$ be the minimal polynomials of $\lambda^{\frac{1}{2}}$ over K. We have that $\deg(\lambda^{\frac{1}{2}}) = \deg(\lambda)$ by Lemma 15, and so $\deg_K(\lambda^{\frac{1}{2}}) = \deg_K(\lambda)$ by Lemmas 14 and 16. Hence $\deg q(x) = \deg p(x)$.

Now $q(x)$ divides the Salem polynomial of $\lambda^{\frac{1}{2}}$, and so the complex roots of $q(x)$ occur in inverse pairs, and the real roots of $q(x)$ are $\lambda^{\frac{1}{2}}$ and possibly $\lambda^{-\frac{1}{2}}$. Now $q(x)$ must have $\lambda^{-\frac{1}{2}}$ as a root, since otherwise the constant term of $q(x)$ would be $-\lambda^{\frac{1}{2}}$ which is not in K, since λ is not in K. Therefore $q(x) = x^m q(x^{-1})$ with $m = \deg q(x)$. Hence $q(x)$ is palindromic.

The roots of $q(-x)$ are distinct from the roots of $q(x)$, since otherwise we would have $q(x) = q(-x)$, since $q(x)$ and $q(-x)$ are irreducible monic polynomials over K, but this is not the case, since $q(x)$ has only positive real roots. As $\pm\lambda^{\frac{1}{2}}$ are roots of $p(x^2)$, we have that $q(x)$ and $q(-x)$ divide $p(x^2)$. Therefore $q(x)q(-x) = p(x^2)$. Hence λ is square-rootable over K via the square 1.

Conversely, assume that λ is square-rootable over K via a square in K. Then there exists a monic palindromic polynomial $q(x)$ over K such that $q(x)q(-x) = p(x^2)$. As $\lambda^{\frac{1}{2}}$ is a root of $p(x^2)$, we have that $\lambda^{\frac{1}{2}}$ is a root of either $q(x)$ or $q(-x)$. By replacing $q(x)$ with $q(-x)$, if necessary, we may assume that $\lambda^{\frac{1}{2}}$ is a root of $q(x)$. Hence the minimal polynomial of $\lambda^{\frac{1}{2}}$ over K divides $q(x)$. Therefore

$$\deg_K(\lambda^{\frac{1}{2}}) \leq \deg q(x) = \deg p(x) = \deg_K(\lambda).$$

Hence $\deg \lambda^{\frac{1}{2}} \leq \deg \lambda$ by Lemmas 14 and 16. Therefore $\deg \lambda^{\frac{1}{2}} = \deg \lambda$ and either $\lambda^{\frac{1}{2}}$ is a Salem number or $\deg \lambda^{\frac{1}{2}} = 2$ and the norm of $\lambda^{\frac{1}{2}}$ is -1 by Lemma 15.

Assume that $\deg \lambda^{\frac{1}{2}} = 2$. Then $\deg \lambda = 2$. We have that $K \subseteq \mathbb{Q}(\lambda + \lambda^{-1}) = \mathbb{Q}$, and so $K = \mathbb{Q}$. Hence $q(x)$ is the minimal polynomial of $\lambda^{\frac{1}{2}}$ over $\mathbb{Q}$. As $q(x)$ is a monic palindromic polynomial, the norm of $\lambda^{\frac{1}{2}}$ is 1. Therefore $\lambda^{\frac{1}{2}}$ must be a Salem number. □

Lemma 18. *Let λ be a Salem number such that $\deg \lambda^{\frac{1}{2}} = 2$ and the norm of $\lambda^{\frac{1}{2}}$ is -1, and let K be a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$. Then λ is square-rootable over K.*

Proof. We have that $\deg \lambda = 2$ and the norm of λ is 1. As $K \subseteq \mathbb{Q}(\lambda + \lambda^{-1}) = \mathbb{Q}$, we have that $K = \mathbb{Q}$. The minimal polynomial of λ over $\mathbb{Q}$ is

$$p(x) = (x - \lambda)(x - \lambda^{-1}) = x^2 - (\lambda + \lambda^{-1})x + 1.$$

We have that $\mathbb{Q}(\lambda^{\frac{1}{2}}) = \mathbb{Q}(\sqrt{D})$ with D a positive square-free integer. Now $\lambda^{\frac{1}{2}} = a + b\sqrt{D}$, with $a, b \in \frac{1}{2}\mathbb{Z}$, and $\lambda^{-\frac{1}{2}} = -a + b\sqrt{D}$. Let $q(x) = (x - \lambda^{\frac{1}{2}})(x - \lambda^{-\frac{1}{2}})$. Then

$$q(x) = x^2 - (\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}})x + 1 = x^2 - 2b\sqrt{D}x + 1$$

and $q(x)q(-x) = p(x^2)$. Hence λ is square-rootable over $\mathbb{Q}$ via D. □

Theorem 7. *Let Γ be an arithmetic group of isometries of hyperbolic n-space H^n, with n odd and $n > 1$, of the simplest type defined over a totally real number field K. Let γ be a hyperbolic element of Γ, and let $\lambda = e^{2\ell(\gamma)}$. Then λ is a Salem number which is square-rootable over K.*

Proof. There exists an admissible quadratic form f over K in $n+1$ variables, and there exists $M \in \mathrm{GL}(n+1, \mathbb{R})$ such that $f(Mx) = f_n(x)$ for all $x \in \mathbb{R}^{n+1}$, and $\Gamma' = M\Gamma M^{-1} \subseteq \mathrm{O}'(f, \mathbb{R})$ with Γ' commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$. Let γ be a hyperbolic element of Γ. Then $\gamma' = M\gamma M^{-1} \in \mathrm{O}'(f, \mathbb{R})$. There exists $B \in \mathrm{GO}(f, K)$ such that $\gamma' = \frac{1}{\sqrt{b}}B$ with $b = \mu(B)$ totally positive by Lemmas 7 and 9. Let $\lambda = e^{2\ell(\gamma)}$. Then $\lambda = e^{\ell(\gamma^2)}$, and so λ is a Salem number with $K \subseteq \mathbb{Q}(\lambda + \lambda^{-1})$ by Lemma 10 and Theorem 4(1).

First assume that b is a square in K. Then γ' is over K, and the same argument as in the proof of Theorem 4(1) shows that $\lambda^{\frac{1}{2}}$ is a Salem number. From the proof of Lemma 17, we deduce that λ is square-rootable over K via b.

Now assume that b is not a square in K. Let $L = K(\sqrt{b})$. Then L is a quadratic extension of K. We have that

$$[L(\lambda^{\frac{1}{2}}) : K] = [L(\lambda^{\frac{1}{2}}) : L][L : K] = 2 \deg_L(\lambda^{\frac{1}{2}}).$$

Now we have that $L(\lambda^{\frac{1}{2}}) = K(\sqrt{b})(\lambda^{\frac{1}{2}}) = K(\lambda^{\frac{1}{2}})(\sqrt{b})$ and

$$[L(\lambda^{\frac{1}{2}}) : K] = [K(\lambda^{\frac{1}{2}})(\sqrt{b}) : K(\lambda^{\frac{1}{2}})][K(\lambda^{\frac{1}{2}}) : K] = \epsilon \deg_K(\lambda^{\frac{1}{2}}),$$

with $\epsilon = 1$ or 2 depending on whether or not $\sqrt{b}$ is in $K(\lambda^{\frac{1}{2}})$. Hence $\deg_L(\lambda^{\frac{1}{2}}) = (1/2)\deg_K(\lambda^{\frac{1}{2}})$ or $\deg_K(\lambda^{\frac{1}{2}})$.

If $\deg \lambda^{\frac{1}{2}} = \deg \lambda$, then λ is square-rootable over K by Lemmas 15, 17, and 18. Hence, we may assume that $\deg \lambda^{\frac{1}{2}} = 2 \deg \lambda$ by Lemma 15. Then $\deg_K(\lambda^{\frac{1}{2}}) = 2\deg_K(\lambda)$ by Lemmas 14 and 16.

Let $p(x)$ and $q(x)$ be the minimal polynomials of λ over K and $\lambda^{\frac{1}{2}}$ over L, respectively. Now γ' is over L. Let $f(x)$ be the characteristic polynomial of γ. Then $f(x)$ is the characteristic polynomial of γ', and so $f(x)$ is over L. The real roots of $f(x)$ are $\lambda^{\pm\frac{1}{2}}$ and possibly ± 1. Hence $q(x)$ divides $f(x)$. Therefore the real roots of $q(x)$ are $\lambda^{\frac{1}{2}}$ and possibly $\lambda^{-\frac{1}{2}}$.

Assume that $\deg_L(\lambda^{\frac{1}{2}}) = \deg_K(\lambda^{\frac{1}{2}})$. Then $\deg_L(\lambda^{\frac{1}{2}}) = 2\deg_K(\lambda)$. As $\lambda^{\frac{1}{2}}$ is a root of $p(x^2)$, we have that $q(x)$ divides $p(x^2)$, and so $q(x) = p(x^2)$, since $\deg q(x) = \deg p(x^2)$. Therefore $-\lambda^{\frac{1}{2}}$ is a root of $q(x)$, which is a contradiction, since the real roots of $q(x)$ are positive. Thus we must have

$$\deg_L(\lambda^{\frac{1}{2}}) = (1/2)\deg_K(\lambda^{\frac{1}{2}}) = \deg_K(\lambda).$$

As $p(x)$ divides the Salem polynomial of λ, the complex roots of $p(x)$ occur in inverse pairs. Now $p(x)$ must have λ^{-1} as a root, since otherwise the constant term of $p(x)$ would be $-\lambda$ which is not in K. Therefore $\deg_K(\lambda)$ is even, and so $\deg_L(\lambda^{\frac{1}{2}})$ is even. As $q(x)$ divides $f(x)$, the complex roots of $q(x)$ occur in inverse pairs. Hence the real roots of $q(x)$ must be $\lambda^{\pm\frac{1}{2}}$. Therefore $q(x) = x^m q(x^{-1})$ with $m = \deg q(x)$, and so $q(x)$ is palindromic.

The roots of $q(-x)$ are distinct from the roots of $q(x)$, since otherwise $q(x)$ and $q(-x)$ would be minimal polynomials over L for a common root, but then we would have $q(x) = q(-x)$, but this is not the case, since $q(x)$ has only positive real roots. As $\pm\lambda^{\frac{1}{2}}$ are roots of $p(x^2)$, we have that $q(x)$ and $q(-x)$ divide $p(x^2)$, Therefore $q(x)q(-x) = p(x^2)$.

Every element of L is of the form $a + c\sqrt{b}$ with $a, c \in K$. Let τ be the automorphism of L over K defined by $\tau(a + c\sqrt{b}) = a - c\sqrt{b}$. Now $q(x)q^\tau(x)$ is over K, and so $q(x)q^\tau(x) = p(x^2)$, since $p(x^2)$ is the minimal polynomial of $\lambda^{\frac{1}{2}}$ over K. Therefore $q^\tau(x) = q(-x)$. Hence the even degree coefficients of $q(x)$ are in K and the odd degree coefficients of $q(x)$ are in $\sqrt{b}K$. Therefore λ is square-rootable over K via b. □

Theorem 8. *Let λ be a Salem number, let K be a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, and let n be an odd positive integer such that $\deg_K(\lambda) \leq n+1$. If λ is square-rootable over K, then there exists an arithmetic group Γ of isometries of H^n of the simplest type defined over K and an orientation preserving hyperbolic element γ in Γ such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$.*

Proof. Let $p(x)$ be the minimal polynomial of λ over K. As $p(x)$ divides the Salem polynomial of λ, the complex roots of $p(x)$ occur in inverse pairs. Therefore $p(x)$ has λ^{-1} as a root, since otherwise the constant term of $p(x)$ would be $-\lambda$ which is not in K. Hence $m = \deg p(x)$ is even.

Assume that λ is square-rootable over K. Then there exists a totally positive element α of K and a monic palindromic polynomial $q(x)$, whose even degree coefficients are in K and whose odd degree coefficients are in $\sqrt{\alpha}K$, such that $q(x)q(-x) = p(x^2)$. Then $\deg q(x) = \deg p(x) = m$. As $\lambda^{\frac{1}{2}}$ is a root of $p(x^2)$, we have that $\lambda^{\frac{1}{2}}$ is a root of either $q(x)$ or $q(-x)$. By replacing $q(x)$ with $q(-x)$, if necessary, we may assume that $\lambda^{\frac{1}{2}}$ is a root of $q(x)$.

The roots of $p(x^2)$ are of the form $\pm r^{\frac{1}{2}}$ where r is a root of $p(x)$. Hence the complex roots of $p(x^2)$ have absolute value 1, and so occur in inverse pairs. Therefore the complex roots of $q(x)$ occur in inverse pairs. The real roots of $p(x^2)$ are $\lambda^{\pm\frac{1}{2}}$ and $-\lambda^{\pm\frac{1}{2}}$. The constant term of $q(x)$ is 1, since $q(x)$ is monic and palindromic. Therefore $q(x)$ has $\lambda^{-\frac{1}{2}}$ as a root, and so the real roots of $q(x)$ are $\lambda^{\pm\frac{1}{2}}$.

Assume that $\lambda^{\frac{1}{2}}$ is a Salem number. Then $\deg\lambda^{\frac{1}{2}} = \deg\lambda$ by Lemma 15, and so $\deg_K(\lambda^{\frac{1}{2}}) = \deg_K(\lambda)$ by Lemmas 14 and 16. Hence $\deg_K(\lambda^{\frac{1}{2}}) \leq n+1$. We have that $K \subseteq \mathbb{Q}(\lambda + \lambda^{-1}) \subseteq \mathbb{Q}(\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}})$. Hence there exists an arithmetic group

Γ of isometries of H^n of the simplest type over K and an orientation preserving hyperbolic element γ in Γ such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$ by Theorem 6.

Thus we may assume that $\lambda^{\frac{1}{2}}$ is not a Salem number. Then α is not a square in K by Lemma 17. Therefore $L = K(\sqrt{\alpha})$ is a quadratic extension of K. Let $q(x) = a_0 + a_1x + \cdots + a_mx^m$, and let $\ell = m/2$. Then $a_{2j} \in K$ for $j = 0, \ldots, \ell$ and $a_{2j-1} \in \sqrt{\alpha}K$ for $j = 1, \ldots, \ell$. Let $b_{2j-1} = a_{2j-1}/\sqrt{\alpha}$ for $j = 1, \ldots, \ell$. Then $b_{2j-1} \in K$ for $j = 1, \ldots, \ell$. As $q(\lambda^{\frac{1}{2}}) = 0$, we have that

$$\sqrt{\alpha}\big(b_1\lambda^{\frac{1}{2}} + b_3\lambda^{\frac{3}{2}} + \cdots + b_{m-1}\lambda^{\frac{m-1}{2}}\big) = -\big(a_0 + a_2\lambda + \cdots + a_m\lambda^{\ell}\big).$$

Now $a_0 + a_2\lambda + \cdots + a_m\lambda^\ell \neq 0$, since $\ell < m = \deg p(x)$. Therefore $\sqrt{\alpha} \in K(\lambda^{\frac{1}{2}})$, and so L is a subfield of $K(\lambda^{\frac{1}{2}})$.

Next we show that the roots of $p(x^2)$ are distinct. Assume first that $\deg \lambda^{\frac{1}{2}} = \deg \lambda$. As $\lambda^{\frac{1}{2}}$ is not a Salem number, $\deg \lambda^{\frac{1}{2}} = 2$ and the norm of $\lambda^{\frac{1}{2}}$ is -1 by Lemma 15. Then $\deg \lambda = 2$. As $K \subseteq \mathbb{Q}(\lambda + \lambda^{-1}) = \mathbb{Q}$, we have that $K = \mathbb{Q}$. Therefore $\deg p(x) = 2$, and so the roots of $p(x^2)$ are $\lambda^{\pm\frac{1}{2}}$ and $-\lambda^{\pm\frac{1}{2}}$. Hence the roots of $p(x^2)$ are distinct. Now assume that $\deg \lambda^{\frac{1}{2}} \neq \deg \lambda$. Then $\deg \lambda^{\frac{1}{2}} = 2 \deg \lambda$ by Lemma 15. Hence $\deg_K(\lambda^{\frac{1}{2}}) = 2\deg_K(\lambda)$ by Lemmas 14 and 16. Therefore $p(x^2)$ is the minimal polynomial of $\lambda^{\frac{1}{2}}$ over K. Hence the roots of $p(x^2)$ are distinct. In either case, we have that the roots of $q(x)$ are distinct.

Let $s_1, s_2, \ldots, s_{m-1} = \lambda^{-\frac{1}{2}}, s_m = \lambda^{\frac{1}{2}}$ be the roots of $q(x)$ taken with $s_{2j} = \overline{s}_{2j-1}$ of absolute value 1. Say $s_{2j} = e^{i\theta_j}$, for $j = 1, \ldots, \ell - 1$, and $s_m = \lambda^{\frac{1}{2}} = e^{\eta}$. Then the roots of $q(-x)$ are $-s_1, \ldots, -s_m$. As $s_1, \ldots, s_m, -s_1, \ldots, -s_m$ are the distinct roots of $p(x^2)$, the distinct roots of $p(x)$ are $r_k = s_k^2$ for $k = 1, \ldots, m$. Now $r_{2j} = e^{i2\theta_j}$ for $j = 1, \ldots, \ell - 1$ and $r_m = \lambda = e^{2\eta}$.

Let $S = \mathrm{diag}(s_1, s_2, \ldots, s_m)$ and let B be the $m \times m$ block diagonal matrix with the first $m - 1$ blocks

$$\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} \quad \text{and last block} \quad \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Then $M = B^{-1}SB$ is the block diagonal $m \times m$ matrix with blocks

$$\begin{pmatrix} \cos\theta_j & -\sin\theta_j \\ \sin\theta_j & \cos\theta_j \end{pmatrix} \quad \text{for} \quad 1 \leq j < \ell, \quad \text{and} \quad \begin{pmatrix} \cosh\eta & \sinh\eta \\ \sinh\eta & \cosh\eta \end{pmatrix}.$$

The matrix M represents a hyperbolic element of $\mathrm{O}'(m-1,1)$ with characteristic polynomial $q(x)$, since the eigenvalues of M are $e^{\pm i\theta_1}, \ldots, e^{\pm i\theta_{\ell-1}}$ and $e^{\pm\eta}$. Moreover $\det M = 1$, and so M represents an orientation preserving isometry of H^n.

Let $V = (v_{ij}) = (r_i^{j-1})$ be the Vandermonde matrix for the roots of $p(x)$. Then V is invertible, since the roots of $p(x)$ are distinct. Let $R = \mathrm{diag}(r_1, \ldots, r_m)$. Then $R = S^2$. Let C be the companion matrix for $p(x)$. Then C is over $\mathfrak{o}_K$ and $VC = RV$. Let $D = V^{-1}SV$. Then $D^2 = V^{-1}RV = C$. Let $W = B^{-1}V$. Then

$$WDW^{-1} = (B^{-1}V)(V^{-1}SV)(B^{-1}V)^{-1} = B^{-1}SB = M.$$

Let J be the $m \times m$ matrix $\mathrm{diag}(1, \ldots, 1, -1)$. Then $M^tJM = J$. Let $A = W^tJW$. Then A is a symmetric $m \times m$ matrix, and as in the proof of Theorem 6, we have that $A = (\sum_{k=1}^m r_k^{i-j}/2)$ and $2A$ is over $\mathfrak{o}_K$. Now A is the coefficient matrix of a quadratic form f over K in m variables. If $x \in \mathbb{R}^m$, then

$$f(x) = x^tAx = x^tW^tJWx = (Wx)^tJWx = f_{m-1}(Wx),$$

and so f has signature $(m-1,1)$ and

$$\mathrm{O}'(f,\mathbb{R}) = W^{-1}\mathrm{O}'(m-1,1)W.$$

Now $M \in \mathrm{O}'(m-1,1)$ and $D = W^{-1}MW$. Hence $D \in \mathrm{O}'(f,\mathbb{R})$. The quadratic form f is admissible by the same argument as in the proof of Theorem 6. Note that as $C = D^2$, the matrix M^2 plays the role of M in the proof of Theorem 6.

We next show that the matrix $\sqrt{\alpha}D$ is over K by a Galois group argument. Let $\hat{K} = K(s_1,\ldots,s_m)$ be the splitting field of $p(x^2)$ over K, and let $G = \mathrm{Gal}(\hat{K}/K)$. As L is a quadratic extension of K contained in $\hat{K}$, there is an index 2 subgroup H of G such that $H = \mathrm{Gal}(\hat{K}/L)$ by Theorem 3 on p 196 of [17]. Now $\hat{K}$ is also the splitting field of $q(x)$ over L, and so H is the Galois group of $q(x)$. Hence all the elements of H permute the roots $s_1,\ldots,s_m$ of $q(x)$ among themselves.

Every element of L is of the form $a + c\sqrt{\alpha}$ with $a, c \in K$. Let τ be the automorphism of L over K defined by $\tau(a + c\sqrt{\alpha}) = a - c\sqrt{\alpha}$. Then τ extends to an automorphism $\hat{\tau}$ of $\hat{K}$. Observe that

$$\prod_{j=1}^{m}(x - \hat{\tau}(s_j)) = q^{\tau}(x) = q(-x) = \prod_{j=1}^{m}(x + s_j).$$

Hence we have that $\hat{\tau}(\{s_1,\ldots,s_m\}) = \{-s_1,\ldots,-s_m\}$. Let $\sigma \in G$. If $\sigma \in H\hat{\tau}$, then σ extends τ and $\sigma(\{s_1,\ldots,s_m\}) = \{-s_1,\ldots,-s_m\}$. Let π_σ be the permutation of the indices $1,\ldots,m$ such that $\sigma(s_k) = \pm s_{\pi_\sigma(k)}$ for all $k = 1,\ldots,m$, with the plus sign if and only if $\sigma \in H$. Then $\sigma(r_k) = \sigma(s_k^2) = s_{\pi_\sigma(k)}^2 = r_{\pi_\sigma(k)}$, and so σ acts on the roots of $p(x)$ via π_σ. Hence

$$V^{\sigma} = (\sigma(v_{ij})) = (\sigma(r_i^{j-1})) = (r_{\pi_\sigma(i)}^{j-1}) = (v_{\pi_\sigma(i),j}),$$

that is, σ acts on V by permuting rows via π_σ. But then σ acts on V^{-1} by permuting columns via π_σ. Let $V^{-1} = T = (t_{ij})$. Then $T^{\sigma} = (t_{i,\pi_\sigma(j)})$.

Now $D = V^{-1}SV$, and so the ij-entry of D is $d_{ij} = \sum_{k=1}^{m} t_{ik}s_kv_{kj}$. Then

$$\sigma(d_{ij}) = \sum_{k=1}^{m} t_{i,\pi_\sigma(k)}(\pm s_{\pi_\sigma(k)})v_{\pi_\sigma(k),j} = \pm d_{ij}$$

with the plus sign if and only if $\sigma \in H$. Hence $(\sqrt{\alpha}D)^{\sigma} = \sqrt{\alpha}D$ for all $\sigma \in G$, and therefore $\sqrt{\alpha}D$ is over K.

Let m be a positive integer such that $B = m\sqrt{\alpha}D$ is over $\mathfrak{o}_K$. Then $\det B = m^m\alpha^{\frac{m}{2}}$. Let $b = m^2\alpha$. Then $b^{\frac{m}{2}} = \det B$ is in $\mathfrak{o}_K$. Hence $b \in \mathbb{A} \cap K = \mathfrak{o}_k$. We have that $\frac{1}{\sqrt{b}}B = D$, and so $B^2 = bD^2 = bC$.

Let Φ be the congruence b subgroup of $\mathrm{O}'(f,\mathfrak{o}_k)$. Then Φ is a normal subgroup of $\mathrm{O}'(f,\mathfrak{o}_k)$ of finite index, since the quotient ring $\mathfrak{o}_K/(b)$ is finite (cf. [21] p 56).

Let Ψ be the subgroup of $\mathrm{O}'(f,\mathbb{R})$ generated by C and the elements of Φ and $D\Phi D^{-1}$. We claim that Ψ is a subgroup of $\mathrm{O}'(f,\mathfrak{o}_k)$. First of all, $C \in \mathrm{O}'(f,\mathfrak{o}_k)$. Let $X \in \Phi$. Then $DXD^{-1} = DXDC^{-1}$. Now BXB is congruent modulo b to $B^2 = bC$, and so $DXD = BXB/b$ is over $\mathfrak{o}_k$. Hence $DXD^{-1} \in \mathrm{O}'(f,\mathfrak{o}_k)$. Therefore $D\Phi D^{-1}$ is a subgroup of $\mathrm{O}'(f,\mathfrak{o}_k)$, and so Ψ is a subgroup of $\mathrm{O}'(f,\mathfrak{o}_k)$.

Let Δ be the subgroup of $\mathrm{O}'(f,\mathbb{R})$ generated by D and the elements of Ψ. We claim that Ψ is a normal subgroup of Δ. It suffices to show that $D\Psi D^{-1} = \Psi$. As $C = D^2$, we have that $DCD^{-1} = C$. Now $D(D\Phi D^{-1})D^{-1} = C\Phi C^{-1} = \Phi$, since Φ is a normal subgroup of $\mathrm{O}'(f,\mathfrak{o}_k)$. Therefore D conjugates the set of generators of Ψ to itself. Hence $D\Psi D^{-1} = \Psi$, and so Ψ is a normal subgroup of Δ.

Now D is not over K, and so D is not in Ψ. Hence Ψ is a subgroup of index 2 in Δ, since $D^2 = C$ is in Ψ. Moreover $\Delta \cap \mathrm{O}'(f, \mathfrak{o}_k) = \Psi$. We have that Ψ has finite index in $\mathrm{O}'(f, \mathfrak{o}_k)$. Therefore Δ is commensurable to $\mathrm{O}'(f, \mathfrak{o}_k)$. Hence $\Gamma = W\Delta W^{-1}$ is an arithmetic group of isometries of H^{m-1} of the simplest type defined over K. We have that $\gamma = M = WDW^{-1}$ is an orientation preserving hyperbolic element of Γ such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$. If $n = m-1$, we are done, so assume that $n > m-1$.

Consider the following 2×2 matrices

$$D_1 = \begin{pmatrix} 0 & -\sqrt{\alpha} \\ \frac{1}{\sqrt{\alpha}} & 0 \end{pmatrix},\ C_1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ A_1 = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix},$$

$$W_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\alpha} \end{pmatrix},\ J_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ M_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

If X is an $m \times m$ matrix, let $\hat{X}$ be the block diagonal $(n+1) \times (n+1)$ matrix with $(n+1-m)/2$ blocks of the form X_1 and final block X. Then $\hat{D}^2 = \hat{C}$. Now $\hat{A}$ is a symmetric $(n+1) \times (n+1)$ matrix such that $\hat{A} = \hat{W}^t \hat{J} \hat{W}$. Hence $\hat{A}$ is the coefficient matrix of a quadratic form $\hat{f}$ over K in $n+1$ variables of signature $(n, 1)$ with $\mathrm{O}'(\hat{f}, \mathbb{R}) = \hat{W}^{-1}\mathrm{O}'(n,1)\hat{W}$. Moreover $\hat{f}$ is admissible, since f is admissible and α is totally positive. We have that $\hat{D}^t \hat{A} \hat{D} = \hat{A}$ and $\hat{W}\hat{D}\hat{W}^{-1} = \hat{M}$, and so $\hat{D}$ is in $\mathrm{O}'(\hat{f}, \mathbb{R})$. Moreover $\sqrt{\alpha}\hat{D}$ is over K.

Let $\hat{m}$ be a positive integer such that $\hat{m}\sqrt{\alpha}\hat{D}$ is over $\mathfrak{o}_K$, and let $\hat{b} = \hat{m}^2\alpha$. Then as above, $\hat{b} \in \mathfrak{o}_K$. Let $\hat{\Phi}$ be the congruence $\hat{b}$ subgroup of $\mathrm{O}'(\hat{f}, \mathfrak{o}_K)$, let $\hat{\Psi}$ be the subgroup of $\mathrm{O}'(\hat{f}, \mathbb{R})$ generated by $\hat{C}$ and the elements of $\hat{\Phi}$ and $\hat{D}\hat{\Phi}\hat{D}^{-1}$, and let $\hat{\Delta}$ be the subgroup of $\mathrm{O}'(\hat{f}, \mathbb{R})$ generated by $\hat{D}$ and the elements of $\hat{\Psi}$. Then as above, $\hat{\Delta}$ is commensurable to $\mathrm{O}'(\hat{f}, \mathfrak{o}_K)$. Hence $\hat{\Gamma} = \hat{W}\hat{\Delta}\hat{W}^{-1}$ is an arithmetic group of isometries of H^n of the simplest type defined over K. We have that $\hat{\gamma} = \hat{M} = \hat{W}\hat{D}\hat{W}^{-1}$ is an orientation preserving hyperbolic element of $\hat{\Gamma}$ such that $\lambda^{\frac{1}{2}} = e^{\ell(\hat{\gamma})}$. □

The next corollary is an enhanced version of Corollary 3.

Corollary 7. *Let λ be a Salem number. Then for each odd integer $n > 0$, there exists an arithmetic group Γ of isometries of H^n of the simplest type defined over $\mathbb{Q}(\lambda + \lambda^{-1})$ and an orientation preserving hyperbolic element γ of Γ such that γ^4 is a hyperbolic translation and $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$.*

Proof. Let $K = \mathbb{Q}(\lambda + \lambda^{-1})$. Then the minimal polynomial of λ over K is

$$p(x) = (x - \lambda)(x - \lambda^{-1}) = x^2 - (\lambda + \lambda^{-1})x + 1.$$

Hence $\deg_K(\lambda) = 2$, and so $\deg_K(\lambda) \leq n+1$ for each odd positive integer n. Let

$$q(x) = (x - \lambda^{\frac{1}{2}})(x - \lambda^{-\frac{1}{2}}) = x^2 - (\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}})x + 1.$$

Then $q(x)q(-x) = p(x^2)$. Let $\alpha = (\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}})^2 = \lambda + 2 + \lambda^{-1}$. Then $\alpha \in \mathfrak{o}_K$ and $q(x) = x^2 - \sqrt{\alpha}\,x + 1$. Now α is totally positive, since if $\sigma : K \to \mathbb{R}$ is a nonidentity field embedding, then $\sigma(\lambda + \lambda^{-1}) = 2\cos\theta$ for some real number θ such that $0 < \theta < \pi$ by the proof of Lemma 4. Hence λ is square-rootable over K via $\lambda + \lambda^{-1} + 2$. Therefore there exists an arithmetic group Γ of isometries of H^n of the simplest type over K and an orientation preserving hyperbolic element γ of Γ

such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$ by Theorem 8. Moreover γ^4 is a hyperbolic translation by the proof of Theorem 8, since $\deg(p(x)) = 2$. $\square$

For example when $n = 1$ in Corollary 7, the proof of Theorem 8 yields

$$A = \tfrac{1}{2}\begin{pmatrix} 2 & \lambda+\lambda^{-1} \\ \lambda+\lambda^{-1} & 2 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -1 \\ 1 & \lambda+\lambda^{-1} \end{pmatrix}, \quad V = \begin{pmatrix} 1 & \lambda^{-1} \\ 1 & \lambda \end{pmatrix}$$

with A the coefficient matrix of the binary quadratic form

$$f(x) = x_1^2 + (\lambda+\lambda^{-1})x_1x_2 + x_2^2$$

and C the companion matrix to the minimal polynomial of λ over $K = \mathbb{Q}(\lambda+\lambda^{-1})$, and V the Vandermonde matrix for roots λ^{-1} and λ. Let $\alpha = \lambda + \lambda^{-1} + 2$. Then we have

$$D = V^{-1}\mathrm{diag}(\lambda^{-1/2}, \lambda^{1/2})V = \frac{1}{\sqrt{\alpha}}\begin{pmatrix} 1 & -1 \\ 1 & \lambda+\lambda^{-1}+1 \end{pmatrix}$$

with $D \in \mathrm{O}'(f, \mathbb{R})$ and $D^2 = C$, and $\sqrt{\alpha}D$ and C matrices over $\mathfrak{o}_K$. Clearly, the eigenvalues of D are $\lambda^{1/2}$ and $\lambda^{-1/2}$. We have that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$ for $\gamma = WDW^{-1}$.

The next corollary follows from Theorems 7 and 8.

Corollary 8. *Let Γ be an arithmetic group of isometries of H^n of the simplest type defined over $\mathbb{Q}$, with n odd, and let C be a closed geodesic in H^n/Γ. Then* $\mathrm{length}(C) \geq c_n$*, and this lower bound is sharp for each odd integer $n > 1$.*

Corollary 4 follows from Corollary 8 once we have a sharp non-cocompact example for $n = 3$, since all arithmetic groups of isometries of H^n of the simplest type over $\mathbb{Q}$ are not cocompact when $n > 3$. Such an example will be described in the next section.

9. The values of b_n and c_n for small n

Let $\lambda_{m,\ell}$ be the ℓth largest Salem number of degree m listed in [22]. Lehmer determined the smallest Salem numbers of degree $d = 2, \ldots, 10$ in [18]. The corresponding Salem polynomials and Salem numbers are

$$\begin{array}{lllr} x^2 - 3x + 1, & \lambda_{2,1} & = & 2.6180339887\ldots \\ x^4 - x^3 - x^2 - x + 1, & \lambda_{4,1} & = & 1.7220838057\ldots \\ x^6 - x^4 - x^3 - x^2 + 1, & \lambda_{6,1} & = & 1.4012683679\ldots \\ x^8 - x^5 - x^4 - x^3 + 1, & \lambda_{8,1} & = & 1.2806381562\ldots \\ x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1, & \lambda_{10,1} & = & 1.1762808182\ldots \end{array}$$

Recall that

$$b_n = \min\{\log\lambda : \lambda \text{ is a Salem number with } \deg\lambda \leq n+1\}.$$

From the values of the smallest Salem numbers of degree $d = 2, \ldots, 10$, we derive

$$\begin{array}{lllll} b_1 & = & b_2 & = & 0.9624236501\ldots \\ b_3 & = & b_4 & = & 0.5435350724\ldots \\ b_5 & = & b_6 & = & 0.3373778035\ldots \\ b_7 & = & b_8 & = & 0.2473585132\ldots \\ b_9 & = & b_{10} & = & 0.1623576120\ldots \end{array}$$

The smallest known Salem number is Lehmer's smallest 10th degree Salem number $\lambda_{10,1}$. The values of the smallest Salem numbers of degree at most 44 have been determined [22], and so

$$b_{10} = b_{11} = \cdots = b_{44}.$$

Lemma 19. *Let λ be a Salem number, let K be a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, let $p(x)$ be the minimal polynomial of λ over K, and let $m = \deg p(x)$. Suppose that λ is square-rootable over K via α in K.*

1. *If $m \equiv 0 \bmod 4$, then $p(-1)$ is a square in $\mathfrak{o}_K$.*
2. *If $m \equiv 2 \bmod 4$, then there exists $k \in K^*$ such that $p(-1) = \alpha k^2$.*

Proof. There exists a monic palindromic polynomial $q(x)$, whose even degree coefficients are in K and whose odd degree coefficients are $\sqrt{\alpha}\, K$, such that $q(x)q(-x) = p(x^2)$. Hence $p(-1) = q(i)q(-i)$. We have that

$$q(-i) = q(1/i) = i^{-m} i^m q(1/i) = i^{-m} q(i).$$

Hence we have that $p(-1) = i^{-m} q(i)^2$.

(1) Assume that $m \equiv 0 \bmod 4$. Then $i^m = 1$. Hence $p(-1) = q(i)^2$. If k is an odd positive integer, then $i^{m-k} = i^{-k} = (-i)^k = -i^k$. Hence the odd degree terms of $q(x)$ cancel in the evaluation of $q(i)$. The roots of $q(x)$ are in $\mathbb{A}$, and so the even degree coefficients of $q(x)$ are in $\mathbb{A} \cap K = \mathfrak{o}_K$. Therefore $q(i) \in \mathfrak{o}_K$. Hence $p(-1)$ is a square in $\mathfrak{o}_K$.

(2) Assume that $m \equiv 2 \bmod 4$. Then $i^m = -1$. Hence $p(-1) = -q(i)^2$. If k is an even nonnegative integer, then $i^{m-k} = -i^{-k} = -(-i)^k = -i^k$. Therefore the even degree terms of $q(x)$ cancel in the evaluation of $q(i)$. Hence there exists $k \in K$ such that $q(i) = \sqrt{\alpha}\, k\, i$. Therefore $p(-1) = \alpha k^2$. As $p(-1) \neq 0$, we have that $k \neq 0$. □

Lemma 20. *Let λ be a Salem number, let K be a subfield of $\mathbb{Q}(\lambda + \lambda^{-1})$, and let $p(x)$ be the minimal polynomial of λ over K.*

1. *If $\deg p(x) = 2$, then λ is square-rootable over K via $\lambda + \lambda^{-1} + 2$.*
2. *If $p(x) = x^4 + ax^3 + bx^2 + ax + 1$, then λ is square-rootable over K if and only if there is a positive element k of $\mathfrak{o}_K$ such that $p(-1) = k^2$ and $4 - a \pm 2k$ is a totally positive element of K, in which case λ is square-rootable over K via $4 - a \pm 2k$.*
3. *If $\deg p(x) = 4$ and $K = \mathbb{Q}$, then λ is square-rootable over K if and only if $p(-1)$ is a square in $\mathbb{Z}$.*

Proof. (1) We have that

$$p(x) = (x - \lambda)(x - \lambda^{-1}) = x^2 + (\lambda + \lambda^{-1})x + 1.$$

Hence $\lambda + \lambda^{-1} \in K$, and so $K = \mathbb{Q}(\lambda + \lambda^{-1})$. Therefore λ is square-rootable over K via $\lambda + \lambda^{-1} + 2$ by the proof of Corollary 7.

(2) Suppose that λ is square-rootable over K via α. Then $p(-1) = k^2$ with $k \in \mathfrak{o}_K$ by Lemma 19(1). Now $k \neq 0$, since $p(-1) \neq 0$. By replacing k with $-k$, if necessary, we may assume that $k > 0$. Let

$$q(x) = x^4 + cx^3 + dx^2 + cx + 1$$

such that $q(x)q(-x) = p(x^2)$ with $c = \sqrt{\alpha}\ell$ for some $\ell \in K$ and $d \in K$. Then $2d - c^2 = a$ and $2 - 2c^2 + d^2 = b$. Hence $c^2 = 2d - a$, and so $2 - 4d + 2a + d^2 = b$. Therefore

$$d = 2 \pm \sqrt{2 - 2a + b} = 2 \pm \sqrt{p(-1)} = 2 \pm k$$

and

$$c = \pm\sqrt{2d-a} = \pm\sqrt{4 \pm 2k - a}.$$

As $4 - a \pm 2k = c^2 = \alpha\ell^2$, we have that $4 - a \pm 2k$ is totally positive.

Conversely, if k is a positive element of $\mathfrak{o}_K$ such that $p(-1) = k^2$ and $4-a\pm 2k$ is totally positive, then we can solve for c and d from the above equations and deduce that λ is square-rootable over K via $4 - a \pm 2k$.

(3) By (2) it suffices to show that if λ is square-rootable over $K = \mathbb{Q}$, then $4-a+2k$ is positive. Let $\lambda^{\pm 1}, \mu^{\pm 1}$ be the roots of $p(x)$. Then $-a = \lambda+\lambda^{-1}+\mu+\mu^{-1}$. We have that $\lambda + \lambda^{-1} > 2$ and $\mu + \mu^{-1} = 2\cos\theta$ for some real number θ, and so $-a > 0$. Therefore $4 - a + 2k > 0$. □

Recall that

$$\begin{aligned} c_n \;=\; & \min\{\tfrac{1}{2}\log\lambda : \lambda \text{ is a Salem number with } \deg\lambda \le n+1, \\ & \qquad \text{which is square-rootable over } \mathbb{Q}\}. \end{aligned}$$

It follows from Lemma 20(1) that

$$c_1 = c_2 = \tfrac{1}{2}\log\lambda_{2,1} = 0.481211825\dots\ .$$

The smallest Salem number of degree 4 with Salem polynomial $p(x)$ such that $p(-1)$ is a square in $\mathbb{Z}$ is

$$\lambda_{4,6} = \frac{1}{4}\left(1 + \sqrt{21} + \sqrt{2\big(3+\sqrt{21}\big)}\right) = 2.3692054071\dots$$

with Salem polynomial

$$p(x) = x^4 - x^3 - 3x^2 - x + 1.$$

We have that $p(-1) = 1$, and so $\lambda_{4,6}$ is square-rootable over $\mathbb{Q}$ via 3 and 7 by Lemma 20(2). Hence we have that

$$c_3 = c_4 = \tfrac{1}{2}\log\lambda_{4,6} = 0.4312773138\dots\ .$$

To finish the proof of Corollary 4, we need a non-cocompact arithmetic group Γ of isometries of H^3 and a hyperbolic element γ of Γ such that $\lambda_{4,6} = e^{2\ell(\gamma)}$. The proof of Theorem 8 yields an arithmetic group Γ of isometries of H^3 of the simplest type over $\mathbb{Q}$ and a hyperbolic element γ of Γ such that $\lambda_{4,6} = e^{2\ell(\gamma)}$. A conjugate of Γ is commensurable to $\mathrm{O}'(f,\mathbb{Z})$ where the quadratic form f has coefficient matrix

$$A = \frac{1}{2}\begin{pmatrix} 4 & 1 & 7 & 13 \\ 1 & 4 & 1 & 7 \\ 7 & 1 & 4 & 1 \\ 13 & 7 & 1 & 4 \end{pmatrix}.$$

The only solution of $f(x) \equiv 0 \bmod 7$ with $x \in \mathbb{Z}^4$ is $x \equiv (0,0,0,0) \bmod 7$. Hence, by a descent argument, the only solution of $f(x) = 0$ with $x \in \mathbb{Z}^4$ is $x = (0,0,0,0)$, and so the only solution of $f(x) = 0$ with $x \in \mathbb{Q}^4$ is $x = (0,0,0,0)$. Therefore $\mathrm{O}'(f,\mathbb{Z})$ is cocompact, and so Γ is cocompact, which is not what we need.

Let $K = \mathbb{Q}(\sqrt{-3})$ and let $\omega = (1+i\sqrt{3})/2$. Then $\mathfrak{o}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$. The group $\mathrm{PSL}(2,\mathfrak{o}_K)$ is a noncocompact arithmetic group of isometries of the upper half-space model of hyperbolic 3-space which contains a loxodromic hyperbolic element η represented by the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & \omega \end{pmatrix}.$$

We have that $\lambda_{4,6} = e^{\ell(\eta)}$ (cf. [23] §4). By Theorem 4.11 of [23] there is a subgroup Γ of $\mathrm{PSL}(2,\mathbb{C})$ that is commensurable to $\mathrm{PSL}(2,\mathfrak{o}_K)$ and a hyperbolic element γ of Γ such that $\gamma^2 = \eta$, and so $\lambda_{4,6} = e^{2\ell(\gamma)}$. Thus the bound c_n is sharp in Corollary 4 for $n = 3$. We thank Alan Reid for communicating this example to us.

In order to find the values of c_n for $n > 4$, we need to determine when a Salem number of degree greater than 4 is square-rootable over $\mathbb{Q}$. In this regard, the necessary conditions in Lemma 19 are useful. In practice, we used a more systematic method which we describe next.

Let $p(x)$ be a Salem polynomial for a Salem number λ of degree $m > 4$, and let $\ell = m/2$. Let $r_1, r_1^{-1}, \ldots, r_\ell, r_\ell^{-1}$ be the roots of $p(x)$ with $r_1 = \lambda$. Choose complex numbers $s_1, s_2, \ldots, s_\ell$ so that $s_j^2 = r_j$ for each j and $s_1 = \lambda^{\frac{1}{2}}$. There are two choices for each s_j with $1 < j \leq \ell$ and so there are a total of $2^{\ell-1}$ choices. Let

$$q(x) = (x^2 - (s_1 + s_1^{-1})x + 1)\cdots(x^2 - (s_\ell + s_\ell^{-1})x + 1).$$

Then we have that $q(x)q(-x) = p(x^2)$. In order for λ to be square-rootable over $\mathbb{Q}$, the even degree coefficients of $q(x)$ must be integers and the squares of the odd degree coefficients of $q(x)$ must be integers with the same square-free part for some choice of $s_1, \ldots, s_\ell$. These conditions can be checked numerically.

We determined that the smallest Salem number of degree 6 that is square-rootable over $\mathbb{Q}$ is

$$\lambda_{6,4} = 1.5823471836\ldots$$

with Salem polynomial

$$p(x) = x^6 - x^4 - 2x^3 - x^2 + 1$$

and

$$q(x) = x^6 - \sqrt{2}\,x^5 + x^4 - \sqrt{2}\,x^3 + x^2 - \sqrt{2}\,x + 1.$$

Hence we have that

$$c_5 = c_6 = \tfrac{1}{2}\log\lambda_{6,4} = 0.2294546519\ldots .$$

The smallest Salem number of degree 8 that is square-rootable over $\mathbb{Q}$ is $\lambda_{8,8} = \lambda_{8,1}^2$. As $c_6 < b_8$, we have that $c_6 = c_7 = c_8$.

The smallest Salem number of degree 10 that is square-rootable over $\mathbb{Q}$ is $\lambda_{10,8} = \lambda_{10,1}^2$. Hence we have that

$$c_9 = c_{10} = b_{10} = 0.1623576120\ldots .$$

The smallest Salem number of degree 12 that is square-rootable over $\mathbb{Q}$ is $\lambda_{12,16} = \lambda_{12,1}^2$. Hence we have that $c_{10} = c_{11} = c_{12} = b_{10}$.

The smallest Salem number of degree 14 that is square-rootable over $\mathbb{Q}$ is $\lambda_{14,17} = \lambda_{14,1}^2$. Hence we have that $c_{12} = c_{13} = c_{14} = b_{10}$.

The smallest Salem number of degree 16 that is square-rootable over $\mathbb{Q}$ is

$$\lambda_{16,23} = 1.4908316618\ldots$$

with Salem polynomial

$$p(x) = x^{16} - x^{14} - x^{12} - 2x^{11} - x^8 - 2x^5 - x^4 - x^2 + 1$$

and

$$q(x) = x^{16} - \sqrt{2}\,x^{15} + x^{14} - \sqrt{2}\,x^{13} + x^{12} - x^8 + x^4 - \sqrt{2}\,x^3 + x^2 - \sqrt{2}\,x + 1.$$

We have that $\frac{1}{2}\log\lambda_{16,23} = 0.19966\ldots$, and so we have that $c_{14} = c_{15} = c_{16} = b_{10}$.

The smallest Salem number of degree 18 that is square-rootable over $\mathbb{Q}$ is $\lambda_{18,22} = \lambda_{18,1}^2$. Hence we have that $c_{16} = c_{17} = c_{18} = b_{10}$.

The smallest Salem number of degree 20 that is square-rootable over $\mathbb{Q}$ is $\lambda_{20,74} = \lambda_{20,1}^2$. Hence we have that $c_{18} = c_{19} = c_{20} = b_{10}$.

10. An example with K an intermediate field

All the examples of a Salem number λ that is square-rootable over K that we have considered so far have been with $K = \mathbb{Q}$ or $\mathbb{Q}(\lambda + \lambda^{-1})$. In this section, we consider an example with K an intermediate field between $\mathbb{Q}$ and $\mathbb{Q}(\lambda + \lambda^{-1})$. Consider the polynomial

$$f(x) = x^4 - 4x^3 - 4x^2 + 4x + 1.$$

The polynomial $f(x)$ is irreducible over $\mathbb{Z}$ and has three roots that lie in the open interval $(-2, 2)$ and one root that is greater than 2. Hence $f(x)$ is the trace polynomial of the Salem polynomial

$$p(x) = x^4 f(x + x^{-1}) = x^8 - 4x^7 - 8x^5 - x^4 - 8x^3 - 4x + 1.$$

The corresponding Salem number has value $\lambda = 4.43861\ldots$, and $f(x)$ is the minimal polynomial of

$$\lambda + \lambda^{-1} = 1 + \sqrt{3} + \sqrt{2 + \sqrt{3}} = 4.6639\ldots\ .$$

Now $\lambda^{1/2} = 2.1068\ldots$ has minimal polynomial $p(z^2)$, since $p(x^2)$ is irreducible over $\mathbb{Z}$, and so $\lambda^{1/2}$ is not a Salem number by Lemma 12(1). The polynomial

$$g(x) = f(x^2 - 2) = x^8 - 12x^6 + 44x^4 - 60x^2 + 25$$

is also irreducible over $\mathbb{Z}$. As

$$(\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}})^2 = \lambda + \lambda^{-1} + 2,$$

we have that $g(x)$ is the minimal polynomial of

$$\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}} = \sqrt{3 + \sqrt{3} + \sqrt{2 + \sqrt{3}}} = 2.58145\ldots\ .$$

Now we have the factorizations

$$\begin{aligned} f(x) &= \Big(x^2 - \big(2 + \sqrt{2}\big)x - \big(3 + 2\sqrt{2}\big)\Big)\Big(x^2 - \big(2 - \sqrt{2}\big)x - \big(3 - 2\sqrt{2}\big)\Big) \\ &= \Big(x^2 - \big(2 + 2\sqrt{3}\big)x + \big(2 + \sqrt{3}\big)\Big)\Big(x^2 - \big(2 - 2\sqrt{3}\big)x + \big(2 - \sqrt{3}\big)\Big) \\ &= \Big(x^2 - \big(2 + \sqrt{6}\big)x - 1\Big)\Big(x^2 - \big(2 - \sqrt{6}\big)x - 1\Big) \end{aligned}$$

with $\lambda + \lambda^{-1}$ a root of the first factor in each case. This implies that $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\lambda + \lambda^{-1})$. The polynomial $f(x)$ was carefully chosen so that its Galois group is a Klein four group. Hence the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\lambda + \lambda^{-1})$ are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ corresponding to the three subgroups of $\mathrm{Gal}(f(x))$ of index 2 by Theorem 3 on p 196 of [17].

Let K be one of the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{6})$, and let $f_K(x)$ be the first factor of the above factorization of $f(x)$ over K. Then the minimal polynomial of λ over K is

$$p_K(x) = x^2 f_K(x + x^{-1}).$$

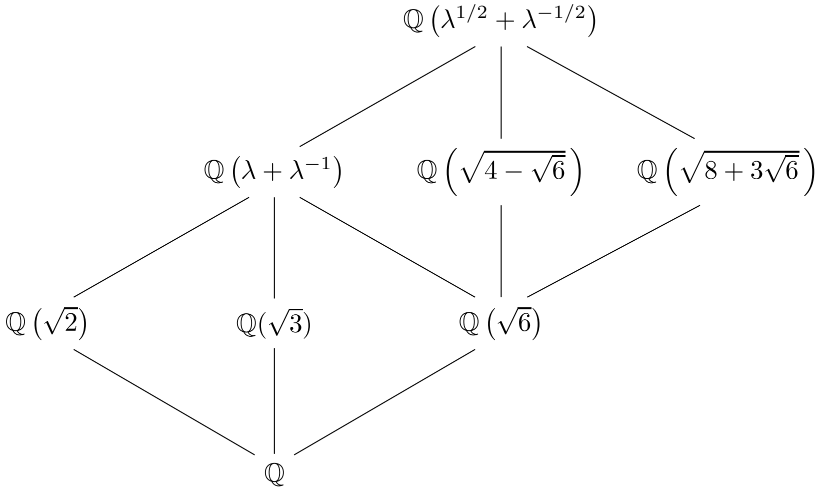
$\mathbb{Q}\left(\lambda^{1/2}+\lambda^{-1/2}\right)$
$\mathbb{Q}\left(\lambda+\lambda^{-1}\right)$
$\mathbb{Q}\left(\sqrt{4-\sqrt{6}}\right)$
$\mathbb{Q}\left(\sqrt{8+3\sqrt{6}}\right)$
$\mathbb{Q}\left(\sqrt{2}\right)$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}\left(\sqrt{6}\right)$
$\mathbb{Q}$

FIGURE 1. Lattice of considered subfields of $\mathbb{Q}(\lambda^{\frac{1}{2}}+\lambda^{-\frac{1}{2}})$

If $K=\mathbb{Q}(\sqrt{2})$, then $p_K(-1)=f_K(-2)=5$, which is not a square in $\mathfrak{o}_K$, and so λ is not square-rootable over $\mathbb{Q}(\sqrt{2})$ by Lemma 20(2). If $K=\mathbb{Q}(\sqrt{3})$, then $p_K(-1)=f_K(-2)=10+5\sqrt{3}$, which is not a square in $\mathfrak{o}_K$, and so λ is not square-rootable over $\mathbb{Q}(\sqrt{3})$ by Lemma 20(2).

Now suppose that $K=\mathbb{Q}(\sqrt{6})$, then

$$p_K(-1)=f_K(-2)=7+2\sqrt{6}=\left(1+\sqrt{6}\right)^2.$$

We have that

$$p_K(x)=x^4-\left(2+\sqrt{6}\right)x^3+x^2-\left(2+\sqrt{6}\right)x+1.$$

Then λ is square-rootable over K via $\alpha=4-\sqrt{6}$ and $\beta=8+3\sqrt{6}$ by Lemma 20(2).

Let $h(x)=x^4-\left(6-\sqrt{6}\right)x^2+\left(7-2\sqrt{6}\right)$. Then we have the factorizations

$$\begin{aligned} g(z) &= \left(x^2-\sqrt{\alpha}\,x-\left(1+\sqrt{6}\right)\right)\left(x^2+\sqrt{\alpha}\,x-\left(1+\sqrt{6}\right)\right)h(x)\\ &= \left(x^2-\sqrt{\beta}\,x+\left(1+\sqrt{6}\right)\right)\left(x^2+\sqrt{\beta}\,x+\left(1+\sqrt{6}\right)\right)h(x)\end{aligned}$$

with $\lambda^{1/2}+\lambda^{-1/2}$ a root of the first factor in each case. This implies that $\sqrt{\alpha},\sqrt{\beta}\in\mathbb{Q}(\lambda^{\frac{1}{2}}+\lambda^{-\frac{1}{2}})$. The lattice of considered subfields of $\mathbb{Q}\left(\lambda^{1/2}+\lambda^{-1/2}\right)$ is shown in Figure 1, with each line indicating a degree 2 extension.

Let $r_1, r_2, r_3=\lambda^{-1}$, and $r_4=\lambda$, be the four roots of $p_K(x)$. Let

$$A=\left(\sum_{k=1}^{4} r_k^{i-j}/2\right).$$

The matrix A is a symmetric function of the roots of $p_K(z)$, and so the entries of A can expressible in terms of the coefficients of $p_K(z)$ by Newton identities, which works out to be

$$A = \frac{1}{2}\begin{pmatrix} 4 & 2+\sqrt{6} & 8+4\sqrt{6} & 44+18\sqrt{6} \\ 2+\sqrt{6} & 4 & 2+\sqrt{6} & 8+4\sqrt{6} \\ 8+4\sqrt{6} & 2+\sqrt{6} & 4 & 2+\sqrt{6} \\ 44+18\sqrt{6} & 8+4\sqrt{6} & 2+\sqrt{6} & 4 \end{pmatrix}.$$

The matrix A has signature $(3, 1)$, and the automorphism of K taking $\sqrt{6}$ to $-\sqrt{6}$ takes A to a positive definite matrix, and so the corresponding quadratic form $f(x) = x^t Ax$ over K is admissible.

Let $L = K(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{\alpha})$. The minimal polynomial of $\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}}$ over L is

$$g_L(x) = x^2 - \sqrt{\alpha}\, x - (1 + \sqrt{6}).$$

The minimal polynomial of $\lambda^{\frac{1}{2}}$ over L is

$$q_L(x) = z^2 g_L(x + x^{-1}) = x^4 - \sqrt{\alpha}\, x^3 + (1 - \sqrt{6})x^2 - \sqrt{\alpha}\, x + 1,$$

and $q_L(x)q_L(-x) = p_K(x^2)$ showing that λ is square-rootable over K via α.

Let $s_1, s_2, s_3 = \lambda^{-1/2}$, and $s_4 = \lambda^{1/2}$ be the roots of $q_L(x)$, taken in order so that $s_k^2 = r_k$ each k. Let V be the Vandermonde matrix (r_i^{j-1}), and let

$$D = V^{-1}\mathrm{diag}(s_1, s_2, s_3, s_4)V.$$

Then we find that

$$D = \frac{1}{5\sqrt{\alpha}}\begin{pmatrix} 6-\sqrt{6} & -1+\sqrt{6} & 1-\sqrt{6} & -6+\sqrt{6} \\ 3-3\sqrt{6} & 2-2\sqrt{6} & 3+2\sqrt{6} & 7+3\sqrt{6} \\ 3+2\sqrt{6} & 2-2\sqrt{6} & 3-3\sqrt{6} & -3+3\sqrt{6} \\ 1-\sqrt{6} & -1+\sqrt{6} & 6-\sqrt{6} & 9+\sqrt{6} \end{pmatrix}$$

with a common denominator of $\sqrt{b}$ for $b = 5^2\alpha$. Then $D \in \mathrm{O}'(f, \mathbb{R})$ and $D^2 = C$ where C is the companion matrix of $p_K(x)$ given by

$$C = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 2+\sqrt{6} \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2+\sqrt{6} \end{pmatrix}.$$

The matrix D is over L, but $\sqrt{b}D$ and C are over $\mathfrak{o}_K$, and so $C \in \mathrm{O}'(f, \mathfrak{o}_K)$. As in the proof of Theorem 8, let Φ be the congruence b subgroup of $\mathrm{O}'(f, \mathfrak{o}_K)$ and let Δ be the subgroup of $\mathrm{O}'(f, \mathbb{R})$ generated by D and Φ. Then Δ is commensurable to $\mathrm{O}'(f, \mathfrak{o}_K)$. Hence $\Gamma = W\Delta W^{-1}$ is an arithmetic group of isometries of H^3 of the simplest type defined over K, and $\gamma = WDW^{-1}$ is an orientation preserving loxodromic hyperbolic element of Γ such that $\lambda^{\frac{1}{2}} = e^{\ell(\gamma)}$.

Likewise for $L = \mathbb{Q}(\sqrt{\beta})$, we derive a similar conclusion with

$$D = \frac{1}{5\sqrt{\beta}}\begin{pmatrix} 4+\sqrt{6} & 1-\sqrt{6} & -1+\sqrt{6} & -4-\sqrt{6} \\ 7+3\sqrt{6} & 8+2\sqrt{6} & -3-2\sqrt{6} & 13+7\sqrt{6} \\ -3-2\sqrt{6} & 8+2\sqrt{6} & 7+3\sqrt{6} & -7-3\sqrt{6} \\ -1+\sqrt{6} & 1-\sqrt{6} & 4+\sqrt{6} & 21+9\sqrt{6} \end{pmatrix}.$$

References

[1] I. Agol, D. D. Long, and A. W. Reid, The Bianchi groups are separable on geometrically finite subgroups, *Ann. Math.* 153 (2001), 599-621.

[2] E. Artin, *Geometric Algebra*, Interscience, New York, 1957.

[3] A. F. Beardon, *The Geometry of Discrete Groups*, Graduate Texts in Math. vol. 91, Springer-Verlag, Berlin, Heidelberg, and New York, 1983.

[4] M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, J. P. Schreiber, *Pisot and Salem Numbers*, Birkhäuser Verlag, Basel, 1992.

[5] A. Borel, Linear Algebraic Groups, *Proc. Symp. Pure Math.* vol. IX (1966), 3-19.

[6] A. Borel, *Introduction aux groupes arithmétiques*, Hermann, Paris, 1969.

[7] A. Borel, *Linear Algebraic Groups, 2nd Ed.* Graduate Texts Math. 126, Springer-Verlag, New York, 1991.

[8] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. Math.* 75 (1962), 485-535.

[9] A. Borel and J.-P. Serre, Théorèmes de finitude en cohomologie galoisienne, *Comment. Math. Helv.* 39 (1964), 111-164.

[10] J. W. S. Cassels, *Rational Quadratic Forms*, Dover Publ., Mineola, New York, 1978.

[11] J. Dieudonné, Sur les multiplicateurs des similitudes, *Rend. Circ. Mat. Palermo* 3 (1955), 398-408.

[12] E. Ghate and E. Hironaka, The arithmetic and geometry of Salem numbers, *Bull. Amer. Math. Soc.* 38 (2001), 293-314.

[13] L. Greenberg, Discrete subgroups of the Lorentz group, *Math. Scand.* 10 (1962), 85-107.

[14] E. Hamilton and A. W. Reid, Eigenvalue fields of hyperbolic orbifolds, *Proc. Amer. Math. Soc.* 132 (2004), 2497-2503.

[15] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, Colloq. Publ. 44, Amer. Math. Soc., Providence, Rhode Island, 1998.

[16] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.* 53 (1857), 173-175.

[17] S. Lang, *Algebra*, Addison-Wesley, Reading MA. 1965.

[18] D. H. Lehmer, Factorization of certain cyclotomic functions, *Ann. Math.* 34 (1933), 461-479.

[19] J.-S. Li and J. J. Millson, On the first Betti number of a hyperbolic manifold with an arithmetic fundamental group, *Duke Math. J.* 71 (1993), 365-401.

[20] C. Maclachlan, Commensurability classes of discrete arithmetic hyperbolic groups, *Groups Geom. Dyn.* 5 (2011), 767-785.

[21] Daniel A. Marcus, *Number Fields*, Universitext, Springer-Verlag, New York, 1977.

[22] M. Mossinghoff, Lehmer's Problem, http://academics.davidson.edu/math/mossinghoff/.

[23] W. D. Neumann and A. W. Reid, Arithmetic of hyperbolic manifolds, In: TOPOLOGY '90, Proceedings of the Research Semester in Low Dimensional Topology at Ohio State University, De Gruyter Verlag, Berlin (1992), 273-310.

[24] K. Nomizu, *Fundamentals of Linear Algebra*, McGraw-Hill, New York, 1966.

[25] C. Pisot, Ein Kriterium für die algebraischen Zahlen, *Math. Z.* 48 (1942), 293-323.

[26] R. Salem, Power series with integral coefficients, *Duke Math. J.* 12 (1945), 153-172.

[27] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, Berlin, 1997.

[28] C. Smyth, Seventy years of Salem numbers, Bull. London Math. Soc. 47 (2015), 379-395.

[29] K. Takeuchi, On a Fuchsian group commensurable with the unimodular group, J. Fac. Sci. Univ. Tokyo, Sec. I. 15 (1968), 107-109.

[30] E. B. Vinberg and O. V. Shvartsman, Discrete groups of motions of spaces of constant curvature, In *Geometry II*, Encyclopaedia Math. Sci. 29, Springer, Berlin (1993), 139-248.

Department of Mathematics, University of Bern, Bern, Switzerland

Department of Mathematics, Vanderbilt University, Nashville, TN 37240

E-mail address: j.g.ratcliffe@vanderbilt.edu